Fairfax Software

Solutions from Fairfax Software

For

Jefferson Parish
Louisiana

Request for Proposals
No. 0438

Merchant Card Payment
Processing Services

Due 3:30 PM CDT
Tuesday May 24, 2022

Submitted by:
Fairfax Software
2005 Pan Am Circle, Suite 110
Tampa, FL 33607

Michael Minter, VP, Sales and Marketing
703-802-1220 x103

FAIRFAXSOFTWARE

TAB A – COVER LETTER

Containing summary of proposer's ability to perform the services described in the RFP and confirms that proposer is willing to perform those services and negotiate a contract with the Parish. The letter shall be signed by a person having authority to negotiate and to commit the proposer to a contract. If proposer is a sole-proprietorship, proposer must include a statement that the company is a sole-proprietorship signed by the owner. If proposer is an agency, corporation, partnership or other legal entity, the president, vice-president, secretary or treasurer, or an authorized agent shall sign the proposal, **and** satisfactory evidence of the authority of the person signing for the agency, corporation, partnership or other legal entity shall be attached to the proposal. A sample corporate resolution may be downloaded from the Purchasing Department webpage of the Jefferson Parish website.

Proposers should exhibit their understanding and approach to the project and address how each element will be accomplished. Proposers are advised that except as otherwise provided by law, all documents submitted to the Parish under this RFP are subject to the Louisiana Public Records Act, LSA-R.S. 44:1 et seq., and may be released when a public records request is made in accordance with the law.

Fairfax Software Response:

May 24, 2022

Sidney Duffy
Jefferson Parish
Department of Purchasing
P.O. Box 9
Gretna, Louisiana 70054

Reference: RFP No.: 0438 to provide Payment Processing Services for Debit/Credit Card and other forms of electronic payments

Dear Ms. Duffy:

Fairfax Imaging, Inc. (dba Fairfax Software) is pleased to submit this proposal to the Jefferson Parish for Payment Processing Services in response to the above referenced Request for Proposal (RFP). We state with confidence that Fairfax Software has addressed all requirements listed in the RFP. The information contained in this proposal or any part thereof, including any exhibits, schedules, and other documents and instruments delivered or to be delivered to the Jefferson Parish is true, accurate, and complete.

Fairfax Software is a corporation founded in the State of Virginia on August 16, 1994. Our worldwide headquarters is at 2005 Pan Am Circle, Suite 110, Tampa, Florida 33607, Tel: 703-802-1220. This is the location that would provide the services related to this project. Our website is www.fairfaxsoftware.com.

Michael Minter is your point of contact and is authorized to sign and bind Fairfax Imaging, Inc. (dba Fairfax Software). Mr. Minter's information is as follows: Vice President, Sales and Marketing, 2005 Pan Am Circle, Suite 110, Tampa, FL 33607, Office: 877-627-8325 x103.
Email: mminter@fairfaxsoftware.com.

We are excited to offer our solution to Jefferson Parish. In fact, today, we proudly proclaim the Parish

as a valued client, whom since 2003 has consistently used our *Quick* Modules platform for the processing of inbound mail (paper) payments received each day. The proposed Fairfax Software solution consists of implementing our *Quick* Payments and *Quick* Modules Cashier product lines which are an extension of the highly successful and award-winning *Quick* Modules platform in use today by the Parish.

As a current provider to the Parish, our solution expands on this platform and offers a fully integrated solution for all payments received at the Parish, inclusive of mail, electronic as well as point of sale (over the counter). This platform hosts the engine that processes the financial transactions at over twenty-four (24) state revenue departments and some of the largest cities and counties in the United States. This highly acclaimed platform is also installed at over one hundred (100) client sites, commercial and governmental alike.

Our proposed solution meets or exceeds all the stated requirements for the Parish. We will provide the services described in the RFP and we confirm our ability and willingness to negotiate a contract with the Parish. Our solution consists of technical attributes not found in other solutions, combined with an experienced team of professionals whom will be dedicated to the configuration and implementation of the solution proposed, along with on-going world class support to maintain the solution to the satisfaction of the Parish.

Fairfax Software will provide a flexible, scalable, configurable system that functions as the primary application for recording payments of all types and in any format remitted to the Parish. Fairfax Software's solution provides centralized payment processing and a SQL database for recording all payment transactions.

Designed and built by Fairfax Software, *Quick* Payments is a fully featured online payment solution that is an extension of our award-winning *Quick* Modules system.

The solution offers several benefits to the Parish including:

- Complete payment lifecycle management
- Payment of one or more invoices as well as setting up scheduled payments for future dates
- Integration with merchant provider and legacy systems
- Comprehensive audit trail features
- Support for electronic payments as well as walk in over the counter payments
- Automatic reconciliation of bank statements
- Automatic email notification of payments submitted
- Complete and integrated reporting for electronic payments; payments received via point-of-sale transactions, and will include the back-office mail payments currently being processed using the *Quick* Modules platform.

Quick Modules Cashier is built on the latest open systems multi-tiered architecture using thin client environment for an exceptional modern look-and-feel customer and user experience. A list of but a few of the technology functions provided within *Quick* Modules Cashier include:

- Modern design that supports touch screen monitors.
- Electronic Check Deposit processing (Check 21)
- A keyboard and mouse are supported but not required.

- Entirely web-based for easy deployment and support.
- Cash drawer support with balancing tools.
- Compatible with virtually all cashiering peripherals.
- Accepts all legal tender including cash, checks, debit cards, credit cards.
- Accepts mobile based digital wallet payments including Apple Pay and Google Pay.
- Card transactions via swipe and EMV chip technology.
- Comprehensive system-wide monitoring dashboard display.
- Complete system reporting tools.
- Secure environment with encryption of data at rest and in transit.
- Standard file structures – no proprietary image formats.
- Library of business rules to select from and ability to create new ones based upon the Parish's business requirements.
- Full featured easy to customize receipt with all transaction details.
- User defined dynamic transaction keys.
- Full accounting, balancing, and reconciliation features.
- Modular in design to add users, processors, workflows, and other applications.
- Full featured data capture including OCR (machine print), ICR (handprint), CAR/LAR, OMR, Barcode 1D, 2D, QR codes.
- Un-throttled processes for recognition allowing maximum productivity.
- Create and maintain retention schedules for all document types.
- On demand retrieval and access of images, files, and data elements

Our integrated solution is entirely authored by Fairfax Software, which owns all the intellectual property rights to all aspects of the solution. We pledge to execute the desire of the Parish as part of this engagement down to the last requirement. We also pledge to provide all the necessary integration points with the Parish applications.

Compliance with industry standards:

Our solution is compliant with most state-of-the-art industry security and accessibility requirements that the Jefferson Parish comes to expect from a professional system of this nature. The proposed solution, which consists of *Quick* Modules Cashier and *Quick* Payments, is PCI-DSS compliant and is required to perform specific compliance audits. It is also SOC 2 Type 1 and Type 2 compliant. Independent auditors have examined our product and performed penetration testing and have approved it for SOC2 Type 2 compliance. In addition, our solution is NIST SP 800-53 compliant, FIPS 140-2 compliant, and ADA 508 compliant.

Implementation Services

We have a strong professional and experienced staff that focus on these payment solutions and have developed a subject matter expertise that is second to none. As such, we are able to accept full responsibility for all the provisions set forth in this RFP without any subcontractors.

With any technology deployment, the approach involves Strategy, People, Process, and Technology to be successful. Our overall strategy involves highly interactive design sessions with the Jefferson Parish to ensure each requirement noted in the RFP is addressed within the system in an approach that is fully understood and agreed upon by all parties. This Business Process Redesign (BPR) effort is essential to our strategy of partnership with the Parish and to provide confidence to the Parish that its requirements are fully understood by Fairfax Software, and the scope covers the needs of the Parish end users.

Fairfax Software's project planning methodology is based on industry best practices and established standards derived from the PMI Institute's Project Management Body of Knowledge (PMBOK). We have adopted and deploy these strategies as part of our project development life cycle, and they have proven successful on projects similar in scope and nature to that of the Parish. Fairfax Software has put together an experienced team of professionals with a high degree of business and technical qualifications and subject matter expertise to implement the proposed system. Our team brings this experience of best practices to the project.

Our approach consists of empowering our Project Manager to be the Parish's best advocate and to make decisions that favor the project. We will also back our Project Manager with a highly qualified Business Analyst who is considered a subject matter expert. Our veteran developers all hold advanced computer science degrees and stand ready to implement any special requirements enunciated by the project's Business Analyst, approved by the Project Manager, and sanctioned by the Parish. Our Quality Assurance Director reports directly to the company's ownership and manages a team that consistently tests and presents its findings independently of the project team.

Each project consists of initiating, planning, executing, controlling/monitoring, and closing phases to provide guidance to the process. Within each of these, specific tasks enacted upon by the Fairfax Software team or provided deliverables ensure a defined approach to the execution of the project.

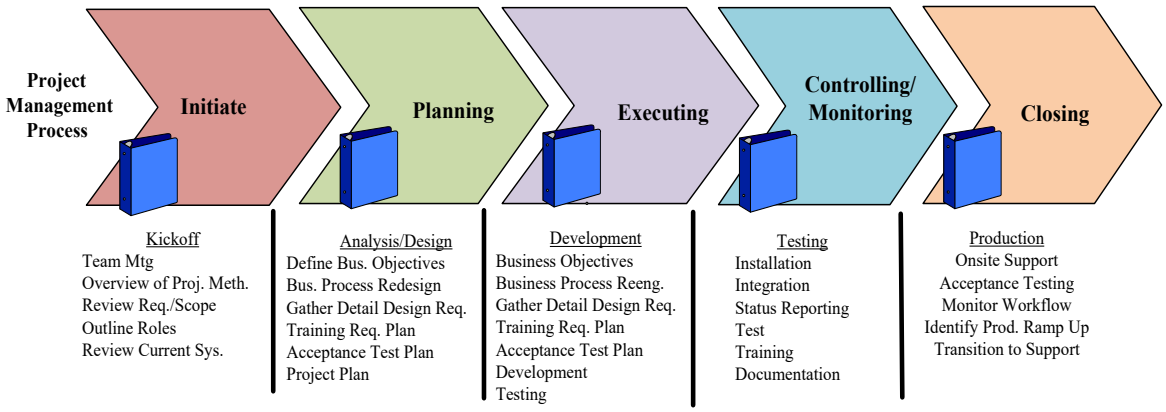


Figure 1 – Project Management Process

Ongoing Maintenance and Support

Fairfax Software fully recognizes that a superior solution will only run better and more optimally when maintained with the pride that the solution maker can provide. Given that every line of code that is featured as part of our offering to the Parish was developed by Fairfax Software engineering staff in-house, we can state with confidence that we are best able to support the solution in-house as well. The support organization does not have to go to a third-party vendor for any requests from the Parish at any time during the expected life of the solution. Instead, it's all in-house: the design, development, testing, and support of our solution. Furthermore, our Support Services Group (SSG) is guided by fundamental standard operating procedures that are clearly understood company wide, and it involves a highly visible ticketing system that provides tracking and accountability for all the staff in the SSG. The issue tracker is visible by the highest level of the executives in the company to ensure total transparency and access to the Parish's immediate feedback. Our offering provides several unique business features which no other

product on the market can match. These include:

No volume or click charges:
The proposed system allows the Parish unlimited use for processing all the daily payment volume. Our system does not include any volume limitations or click charges. Instead, it offers a solution that allows the Parish to grow and expand its reliance on the system without any future licensing charges or fees. Our system will grow in lockstep with the Parish's future needs and requirements without ever a need to count volumes, characters, checks, or any other data capture element.

Single platform:
By adding *Quick* Payments and *Quick* Modules Cashier system to the already installed *Quick* Modules system at the Parish, a streamlined processing environment within a common architecture will be achieved. This singularity eliminates the inherent risks and issues associated with solutions that try to combine these different platforms using different products, companies, and approaches (islands of automation if you will). This unity also offers the Parish the tremendous benefit of consolidated reporting front to back using the same database as the common repository and a common secure infrastructure instead of islands of automation. This benefit to the Parish cannot be understated.

Common library of business rules:
The system is deployed with a library of business rules which can be used for each operational environment, thus providing the Parish with the knowledge that every transaction processed is done so against a set of well-defined rules that ensure data quality and integrity of the system.

Summary
At Fairfax Software we emphasize customer service with a product-dedicated staff of support technicians, ongoing, customer-driven product development, and our "evergreen" software policy that provides software upgrades at no extra charge. This will smooth the migration to a new, enterprise solution that will accommodate Parish-appropriate refinements and ensure the lowest total cost of licensing and support for the Parish throughout the life of the solution.

We take pride in our work, and in our prolific set of references from the most mission-critical accounts in the nation, we also take full responsibility for the planning, development, execution, testing, fielding, and supporting our world-class solution. We will not stop short of an A grade from the Parish in every aspect of our rendering. As you read through the pages of our proposal, you will undoubtedly notice unrivaled subject matter expertise, a great attention to the needs of the Parish, and a very clear depiction of how our technology can serve those needs most effectively. We look forward to your review of our response and to enter into a successful relationship with Jefferson Parish. Should you have any questions about our proposal, please contact me at 877-627-8325 or via email at mminter@fairfaxsoftware.com.

Sincerely

Michael D. Minter
VP, Sales and Marketing

Request for Proposals #0438

Merchant Card Payment Processing Services

SIGNATURE PAGE

The Jefferson Parish Department of Purchasing is soliciting Request for Proposals (RFP'S) from qualified proposers who are interested in providing Merchant Card Payment Processing Services for the Jefferson Parish Finance Department.

Request for Proposals will be received until 3:30 p.m. Local Time on: May, 24, 2022.

Acknowledge Receipt of Addenda: Number: 1
Number: 2
Number:
Number:
Number:
Number:

Name of Proposer: Fairfax Software

Address: 2005 Pan Am Circle, Suite 110

Tampa, FL 33607

Phone Number: 703-802-1220 Fax Number 813-881-1600

Type Name of Person Authorized to Sign: Michael Minter

Title of Person Authorized to Sign: VP, Sales and Marketing

Signature of Person Authorized to Sign: Michael D. Minter

Email Address of Person Authorized to Sign: mminter@fairfaxsoftware.com

Date: May 23, 2022

This RFP signature page must be signed by an authorized Representative of the Company/Firm for proposal to be valid. Signing indicates you have read and comply with the Instructions and Conditions.

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 05/04/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME: Georganna Clark	
Brown & Brown of Florida, Inc. Pinellas Division 83 Park Place Blvd, Suite 101 Clearwater FL 33759	PHONE (A/C, No, Ext): (727) 461-6044	FAX (A/C, No): (727) 442-7695
	E-MAIL ADDRESS: georganna.clark@bbrown.com	

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A :	Atlantic Specialty Insurance Company	27154
INSURER B :	Allied World Assurance Company (U.S.) Inc.	19489
INSURER C :	Great American Alliance Insurance Company	26832
INSURER D :	Travelers Casualty and Surety Co	31194
INSURER E :	Indian Harbor Insurance Company	36940
INSURER F :	Endurance American Specialty	11551

INSURED: Fairfax Imaging, Inc. dba Fairfax Software, 2005 Pan Am Circle, Ste 110, Tampa FL 33607

COVERAGES **CERTIFICATE NUMBER:** CL2182323757 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	[X] COMMERCIAL GENERAL LIABILITY [ ] CLAIMS-MADE [X] OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: [ ] POLICY [ ] PRO-JECT [X] LOC [ ] OTHER:	Y		711-01-59-66-0004	08/29/2021	08/29/2022	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG Employee Benefits	$ 1,000,000 $ 1,000,000 $ 10,000 $ 1,000,000 $ 2,000,000 $ 2,000,000 $ 1,000,000
A	AUTOMOBILE LIABILITY [ ] ANY AUTO [ ] OWNED AUTOS ONLY [ ] SCHEDULED AUTOS [X] HIRED AUTOS ONLY [X] NON-OWNED AUTOS ONLY [X] PIP 10,000			711-01-59-66-0004	08/29/2021	08/29/2022	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident) 	$ 1,000,000 $ $ $ $
A	[X] UMBRELLA LIAB [X] OCCUR EXCESS LIAB [ ] CLAIMS-MADE [ ] DED [X] RETENTION $ 10,000			711-01-59-66-0004	08/29/2021	08/29/2022	EACH OCCURRENCE AGGREGATE 	$ 9,000,000 $ 9,000,000 $
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N: N If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		406-04-47-65-0004	08/29/2021	08/29/2022	[X] PER STATUTE [ ] OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ 1,000,000 $ 1,000,000 $ 1,000,000
B	Primary Cyber			0312-4913	08/29/2021	08/29/2022	Each Occurence	$5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Certificate holder is Additional Insured with respect to General Liability if required by written contract.

CERTIFICATE HOLDER

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

AGENCY CUSTOMER ID: _____

LOC #: _____

ADDITIONAL REMARKS SCHEDULE

Page ____ of ____

AGENCY	NAMED INSURED
Brown & Brown of Florida, Inc.	Fairfax Imaging, Inc. dba Fairfax Software
POLICY NUMBER	
CARRIER / NAIC CODE	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: 25 **FORM TITLE:** Certificate of Liability Insurance: Notes

D&O/EPLI DPLE163957 8/29/2021-8/29/2022
Limits: D&O $2,000,000 Deductible $5,000
EPLI $1,000,000 Deductible $5,000

Crime AGT30988 Travelers Casualty and Surety Co 8/29/2021-8/29/2022
Limits: Each Occurance $1,000,000 Deductible $10,000

Excess Tech E&O/Cyber MTE9035570 04 Indian Harbor Insurance Company 8/29/2021-8/29/2022
Aggregate Limit $5,000,000/Ex $5,000,000

Excess Cyber Liability PVX30010675100 Endurance Assurance Corp 8/29/2021-8/29/2022
Limit Each Claim $5,000,000/Aggregate $5,000,000
Ex Each Claim $10,000,000/Ex Aggregate $10,000,000

Excess Cyber Liability LHZ791286 Landmark American 8/29/2021-8/29/2022
Limit each claim $5,000,000/Ex each Claim $15,000,000
Aggregate Limit $5,000,000/Ex Aggregate $15,000,000

Request for Proposal

AFFIDAVIT

STATE OF Florida

PARISH/COUNTY OF Hillsborough

BEFORE ME, the undersigned authority, personally came and appeared: Michael Minter _____, (Affiant) who after being by me duly sworn, deposed and said that he/she is the fully authorized representative of Fairfax Software (Entity), the party who submitted a proposal in response to RFP Number 0438, to the Parish of Jefferson.

Affiant further said:

Campaign Contribution Disclosures

(Choose A or B, if option A is indicated please include the required attachment):

Choice A _____ Attached hereto is a list of all campaign contributions, including the date and amount of each contribution, made to current or former elected officials of the Parish of Jefferson by Entity, Affiant, and/or officers, directors and owners, including employees, owning 25% or more of the Entity during the two-year period immediately preceding the date of this affidavit or the current term of the elected official, whichever is greater. Further, Entity, Affiant, and/or Entity Owners have not made any contributions to or in support of current or former members of the Jefferson Parish Council or the Jefferson Parish President through or in the name of another person or legal entity, either directly or indirectly.

Choice B XX there are **NO** campaign contributions made which would require disclosure under Choice A of this section.

Affiant further said:

Debt Disclosures

(Choose A or B, if option A is indicated please include the required attachment):

Choice A _____ Attached hereto is a list of all debts owed by the affiant to any elected or appointed official of the Parish of Jefferson, and any and all debts owed by any elected or appointed official of the Parish to the Affiant.

Choice B XX There are **NO** debts which would require disclosure under Choice A of this section.

Affiant further said:

Solicitation of Campaign Contribution Disclosures

(Choose A or B, if option A is indicated please include the required attachment):

Choice A _____ Attached hereto is a list of all elected officials of the Parish of Jefferson, whether still holding office at the time of the affidavit or not, where the elected official, individually, either by **telephone or by personal contact**, solicited a campaign contribution or other monetary consideration from the Entity, including the Entity's officers, directors and owners, and employees owning twenty-five percent (25%) or more of the Entity, during the two-year period immediately preceding the date the affidavit is signed. Further, to the extent known to the Affiant, the date of any such solicitation is included on the attached list.

Choice B XX there are **NO** solicitations for campaign contributions which would require disclosure under Choice A of this section.

Affiant further said:

That Affiant has employed no person, corporation, firm, association, or other organization, either directly or indirectly, to secure the public contract under which he received payment, other than persons regularly employed by the Affiant whose services in connection with the construction, alteration or demolition of the public building or project or in securing the public contract were in the regular course of their duties for Affiant; and

That no part of the contract price received by Affiant was paid or will be paid to any person, corporation, firm, association, or other organization for soliciting the contract, other than the payment of their normal compensation to persons regularly employed by the Affiant whose services in connection with the construction, alteration or demolition of the public building or project were in the regular course of their duties for Affiant.

Affiant further said:

Subcontractor Disclosures

(Choose A or B, if option A is indicated please include the required attachment):

Choice A _____ Affiant further said that attached is a listing of all subcontractors, excluding full time employees, who may assist in providing professional services for the aforementioned RFP.

Choice B XX There are **NO** subcontractors which would require disclosure under Choice A of this section.

Michael D. Minter

Signature of Affiant

Michael D. Minter

Printed Name of Affiant

SWORN AND SUBSCRIBED TO BEFORE ME

ON THE 23 DAY OF May, 2022

Notary Public

Oksana Salem

Printed Name of Notary

GG 201933

Notary/Bar Roll Number

My commission expires July 17, 2022.

OKSANA SALEM
Notary Public - State of Florida
Commission # GG 201933
My Comm. Expires Jul 17, 2022
Bonded through National Notary Assn.

FAIRFAXSOFTWARE

POWER OF ATTORNEY

I, **Steve Chahal**, a Florida resident and the President / Chief Executive Officer of Fairfax Imaging, Inc. (DBA "Fairfax Software"), (hereinafter referred to as "**Fairfax**"), a Virginia Corporation, hereby appoint and constitute **Mr. Michael D. Minter**, (hereinafter referred to as "**Agent**"), as my true and lawful agent and attorney-in-fact, in any and all capacities as President of Fairfax, with full power substitution, for the *limited* purposes of executing on my behalf, such contractual agreements for: (1) the procurement of sales of Fairfax goods and services; and (2) the procurement of third-party vendor goods and services, as Agent deems necessary to carry out the day to day activities of the business of Fairfax in the ordinary course of business.

Termination. This limited power of attorney shall terminate upon the earliest to occur of: (1) any breach by Agent of the limitations of this power of attorney; (2) the termination of Agent's employment with Fairfax; or (3) the termination of this limited power of attorney by Fairfax.

IN WITNESS WHEREOF, the corporation has caused this power of attorney to be executed in its corporate name by its President and Chief Executive Officer this 6th day of January, 2020.

Fairfax Imaging, Inc. (DBA "Fairfax Software"):

By: _____

Steve Chahal
President and Chief Executive Officer

Attorney-in-Fact:

By: Michael D. Minter

Michael D. Minter
Vice President of Sales & Marketing

TAB B -TABLE OF CONTENTS

TAB A-COVER LETTER 1
REQUEST FOR PROPOSAL #0438 SIGNATURE PAGE 6
CERTIFICATE OF INSURANCE—FAIRFAX SOFTWARE 7
REQUEST FOR PROPOSAL #0438 AFFIDAVIT 8
BOD RESOLUTION—FAIRFAX SOFTWARE 10
TAB B-TABLE OF CONTENTS 11
TAB C-TECHNICAL PROPOSAL 12
TAB D-PROPOSER QUALIFICATIONS AND EXPERIENCE 78
TAB E-INNOVATIVE CONCEPTS 85
TAB F—PROJECT SCHEDULE 88
TAB G—FINANCIAL PROFILE 104
ATTACHMENT D—FAIRFAX SOFTWARE REFERENCES 145
ATTACHMENT E-PCI DOCUMENTATION FOR FAIRFAX SOFTWARE 148

TAB C – TECHNICAL PROPOSAL

Illustrating and describing compliance with the RFP requirements defined in the Scope of Work/Services (Part II) and Proposer Qualifications.

2.1 Scope of Work/Services

1. The Merchant service provider (or providers, if multiple contracts are awarded) will be required to provide and operate, consistent with Parish guidelines and oversight, its own front-end payment system to process customer payments for various debt types owed to the Parish.

Fairfax Software Response:

Fairfax Software meets this requirement.

Fairfax Software will provide and operate the *Quick* Payments system consistent with Parish business rules, guidelines, and oversight. The Parish will have control over the system and will maintain ownership of all data processed therein.

2. Online features of the merchant account management software - The vendor should highlight how the merchant account is managed by the accounting/finance functions. For example, describe all the tools and methods for viewing transactions/batches, changing account information, responding to charge backs, user management, etc.

Fairfax Software Response:

Fairfax Software meets this requirement.

Research - Internal Parish users have a full function research tool that allows research by receipt number, customer name, customer number, transaction ID, department, by payment method, by amount, by fee type, and by date range. Users may research credit notes and refunds. Search results may be downloaded as a file in .CSV format.

All research functions are restricted by user privilege. For example, an internal library user can be restricted to library transactions only while an accounting department user can access transactions for all departments.

Refunds and Credit Notes– Refunds are restricted to the original payment type. For example, Mr. Smith paid using a Visa card. Mr. Smith is later approved for a refund; the refund must be deposited back to the Visa card he used from the original transaction. If the original payment type is no longer available, the system will process a credit note. A credit may be used against a future

transaction. *Quick* Payments will be configured to follow Parish business rules regarding refunds and credit notes

Approval Workflow – *Quick* Payments features a built-in approval workflow for refunds and credit notes. For example, a refund must be requested by one internal user and then approved by a supervisor level user before it can be granted. Multiple approval levels are supported. For example, the supervisor level may approve a refund up to $100. Any refunds greater than $100 require a manager's approval.

Chargebacks – Chargebacks are caused by a fraudulent or non-sufficient funds payment. Chargebacks are matched to the original transaction record automatically. Each transaction contains the name and address of the customer making it easier to identify the person for collections.

Reconciliation - *Quick* Payments provides a built-in web-based function to assist the Parish accounting staff with daily management of merchant accounts. With this tool, the time required for account reconciliation is greatly reduced, allowing accounting staff to concentrate on other activities. Here is a brief overview of the process.

- **Input** – In an unattended process, the Input utility will automatically detect when statement files are received electronically from the bank and/or other merchant service providers. Files are verified and strict security measures are followed to ensure the files are genuine before they are copied to a designated folder on the server. Line items are then loaded from the statement file into statement tables within the *Quick* Payments SQL database. This process is automatic and does not require operator intervention.
- **Statement Compare** – Each line item in the statement is compared to the payment database. *Quick* Payments records all matches, mismatches, and non-matches. This process is automatic and does not require operator intervention.
- **Create Report** – The electronic Reconciliation Report is created in PDF format that provides the count and amount of transactions that are reconciled by account and department. The report includes a listing of mismatches and non-matches.
- **Email** - The Reconciliation Report is emailed to the designated accounting personnel. Usually, the automatic reconciliation takes place during off-hours and the reports are ready at the beginning when accounting personnel sign in to begin the workday.
- **Review** - An Internal user selects the Reconciliation button within the internal User screen and reviews all automatic matches/mismatches. A manual matching process is provided to handle any mismatches or non-matches that occur.
- **Output** - Journal entries are automatically generated for Parish accounting systems.

3. Merchant account - management software must be able to identify sub departments in transactions or multiple accounts.

Fairfax Software Response:

Fairfax Software meets this requirement.

Quick Payments reconciliation and account management support sub-departments and multiple accounts. *Quick* Payments can automatically produce multiple general ledger entries per transaction to allocate revenue across multiple accounts and departments.

4. Merchant service provider is asked to provide application programming interface (API) for the debit/credit card processing that is .NET based and can be imbedded in any Jefferson Parish .Net application software.

Fairfax Software Response:

Fairfax Software meets this requirement.

Fairfax Software will provide a .Net-based Application Programming Interface (API) that can be embedded by Parish technical staff into other .Net applications. This will allow existing devices and software to connect to *Quick* Payments in order to process payments.

5. Merchant service provider must also be able to work with other Parish Vendors to develop APIs between their payment system and service delivery or billing software.

Fairfax Software Response:

Fairfax Software meets this requirement.
Quick Payments utilizes web-based APIs to connect with other systems. Fairfax Software will work with other Parish vendors to develop APIs to connect other systems to *Quick* Payments.

6. All software (API) provided must be PCI compliant.

Fairfax Software Response:

Fairfax Software meets this requirement.

Quick Payments and associated APIs are PCI compliant. To connect with *Quick* Payments, other vendors' API's must also be PCI compliant.

7. All payments made by a customer must be immediately deposited directly into a designated Parish bank account through a Parish-approved banking partner, and at no time would flow through the Contractor's bank account.

Fairfax Software Response:

Fairfax Software meets this requirement.

All customer payments are deposited directly into a Parish designated bank account.

2.2 Period of Agreement

The term of any contract shall be for 2 years commencing on date of execution and shall expire 2 years thereafter. The contract may include two 2-year extensions.

Fairfax Software Response:

Fairfax Software agrees to abide by this requirement.

2.3 Cost Proposal (Price Schedule)

Cost proposals must be submitted in separate sealed envelopes which will remain sealed until such time after the evaluation committee makes its evaluation of the proposals on all factors and criteria stated in the RFP. The cost proposals shall not be included in the evaluation criteria. Cost shall be worth twenty-five percent (25%) of the total points assigned. Evaluation of cost shall take place after the technical evaluation has been completed.

Pricing **must** be submitted on the Cost Proposal (Price Schedule) furnished in Attachment B. All proposed pricing shall be inclusive of all additional costs and expenses, including shipment. Prices submitted shall remain firm for the term of the contract, unless otherwise negotiated.

Fairfax Software Response:

The cost proposal has been submitted in a separate electronic envelope.

2.4 Deliverables

The deliverables listed in this section are the minimum desired from the successful proposer. Every proposer must describe what deliverables will be provided per their proposal, and how the proposed deliverables will be provided.

Fairfax Software Response:

The proposed Fairfax Software deliverables are outlined in TAB F – Project Schedule.

2.5 Location

The location(s) where service(s) is/are to be performed are at various Jefferson Parish facilities on both the east and west banks of the parish.

Fairfax Software Response:

Fairfax Software understands this requirement.

2.6 Financial Profile

Proposers are requested to submit documentation from the past 3 years demonstrating proposer's financial stability. Documentation may include audited financial statements including balance sheets, income statements, documentation regarding retained earnings, assets, liabilities, etc. Proposer must include information demonstrating the proposer's financial stability and ability to obtain and maintain bonding and insurance requirements in order to be eligible to be assigned a higher score. Proposals which lack the description of the proposer's financial status, or the required certification of bonding and insurance requirements may be assigned a lower score.

Fairfax Software Response:

The financial profile is included under Tab G – Financial Profile.

2.7 Proposal Elements

A. Technical

1. Each proposer shall address how the proposer will achieve/meet the scope of work as stated in Section 2.1. Technical approach shall detail the following: Plans and/or schedule of implementation, orientation, and/or installation, etc. (whichever is relevant to the RFP requirements)

Fairfax Software Response:

SOLUTION DESCRIPTION

The Fairfax Software *Quick* Payments solution provides a secure and robust online payments solution that meets and exceeds Jefferson Parish's requirements. *Quick* Payments is a modern web application designed to easily integrate with multiple accounting and billing systems using web services APIs. *Quick* Payments is authored by Fairfax Software and provides a single vendor integrated payments solution for the Parish. The Fairfax Software solution includes merchant services from Govolution.

Quick Payments handles all electronic notifications to the citizen as well as relevant Parish staff. Within *Quick* Payments, the Parish has access to unique settings including business rules, bill settings, processing schedules, acceptable payment types, reports, deposit files, operator profiles, automatic bank statement reconciliation, and notification templates. System Templates provide configuration with point-and-click ease - no coding required.

All access is restricted by user login with assigned roles and privileges that restrict what the user may do within the system. Active Directory roles can be used for this purpose or *Quick* Payments can restrict access within the application.

Quick Payments is an extension of the *Quick* Modules system sharing business rules, system workflows, SQL database, reporting, and integrations into the Parish billing and accounting systems. ACH checks are deposited electronically to your bank, Capitol One.

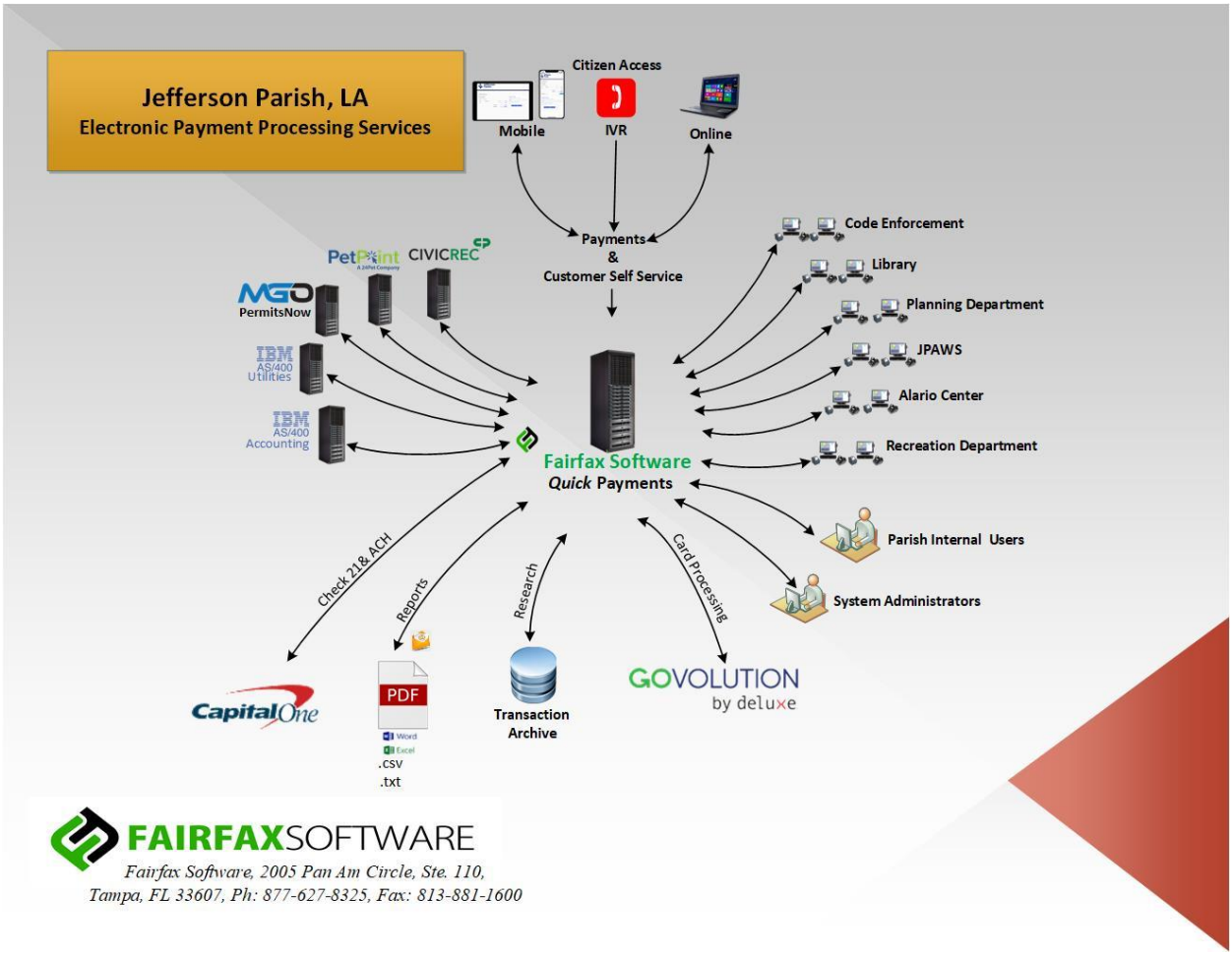


Figure 2 – Cloud based Services

Quick Payments Feature Set

Quick Payments is undeniably the most feature-rich product of its kind in the market. In addition, *Quick* Payments comes out of the box in a standard configurable manner with no programming necessary. The most prominent distinguishing characteristics that set *Quick* Payments apart from the competition are distributed along several attributes. These are:

- ✓ <u>Architectural Attributes:</u>
  1. Service-Oriented Architecture allows integration with external systems via web services APIs.
  2. Web-based for easy deployment and support and providing the Parish with a web interface to take payments, manage configuration and run daily reports.
  3. Deployment in multiple environments – Development, Test, and Production.

4. Three-tier architecture offers many benefits:
   - **Security:** Can be isolated to limit access and exposure.
   - **Availability:** Each tier is independent from the other tiers; this provides the benefit of not having a single point of failure.
   - **Scalability:** Each tier can be scaled as desired without affecting the other tiers.
   - **Flexibility:** Each tier can be managed or scaled independently giving the system increased flexibility.

✓ Security Attributes:

1. Secure PCI and SOC2 compliant environment that has undergone rigorous penetration testing by outside audit entities. Any updates/enhancements do not compromise compliance due to annual penetration testing by outside audit entities.
2. Supports and utilizes secure communications for internet-based transactions.
3. Adheres to Government Accounting Standards Board (GASS) principles as described in http://www.gasb.org/home.
4. Data encryption at rest and in transit following Federal Information Processing Standard (FIPS) Publication 140-2 standards (FIPS PUB 140-2).
5. *Quick* Payments web pages use the HTTPS and over SSL secured network connections.

✓ Ergonomic Attributes:

1. The same consistent straightforward payment experience for all citizens.
2. Special tool for internal users to manage payments, bills, statements, users, user rights, reports, approval workflow, web branding, email templates, system scheduling and other system parameters through the use of a point-and-click system templates.
3. Portal screens are customized to provide a Parish look-and-feel.
4. Creates a real-time electronic receipt that is displayed on the screen, sent via email and/or SMS Text, and can be downloaded in PDF format for printing.
5. Creates payment receipts and supports multiple receipt formats
6. Accepts all US legal tender including cash, checks, debit, and credit cards.
7. Convenience fees (if any) are added to the receipt as a separate line item.
8. Accepts mobile based digital wallet payments i.e., Apple Pay and Google Pay.
9. EMV compliant and support for EMV card processing.

✓ Workflow Attributes:

1. Special tool for internal users to manage payments, bills, statements, users, user rights, reports, approval workflow, web branding, email templates, system scheduling and other system parameters through the use of a point-and-click system templates. Each the Parish departments may have its own unique and personalized setup.
2. An integrated exception processing queue allows users to conduct in-depth research.
3. *Quick* Payments has the option for the Parish to pay the convenience fee or the citizen to pay the convenience fee.
4. Provides comprehensive and separate research features for internal Parish users and citizens.
5. Provides automatic general ledger entries that are included in a file-based transfer to the Parish's accounting systems.
6. Provides automated output of payment files on a schedule set by the Parish. Files are verified before they are sent automatically. Functions are provided to handle

exception conditions.

- ✓ Connectivity Attributes:
  1. Connects to host systems via Web Services APIs or Open Database Connectivity (ODBC) to provide automatic lookup and verification of billing data.
  2. Provides interfaces to backend systems to post payments, void payments, and lookup billing information.
  3. Integrates with the Parish's legacy imaging system (if any).
  4. All card transactions are authorized in real-time regardless of the transaction amount.
- ✓ Audit Tracking Attributes:
  1. Tracking transactions from receipt all the way through the entire processing pipeline to output.
  2. Multilevel approval workflow is available for required processes. For example, approval can be required before a citizen can initiate a payment plan.
  3. Robust comprehensive reporting based on Microsoft SQL Server Reporting Services (SSRS).
  4. Full logging (verbose and summary) capability.
  5. Full audit tracking reporting.
  6. Standard and customized reports.
  7. Maintains the integrity of the database and transactions in case of power failure or abrupt shutdown.
  8. Provides the ability to restart and recover after an abrupt shutdown or power failure without loss of data or software components.
  9. Provides a full audit trail of all transactions, record changes and user logins.
  10. Provides the ability to re-print receipts. All re-printed receipts are identified as a duplicate/re-print of the original.
  11. Provides a method to reverse transactions including integrated systems.
  12. Provides a method, controlled through security, of correcting or adjusting a transaction previously posted. Allows the operator to alter/update fields, issue a void of the original transaction and post the new transaction to keep the audit trail intact.
  13. Allow all reports to be exported in common formats including but not limited to, Microsoft Excel, Microsoft Word, Adobe PDF, Comma Separated Values (CSV), Extensible Markup Language (XML), fixed field text (TXT), JavaScript Object Notation (JSON).
  14. Provides payment statistics. For example, number of payments processed in a given time, number of payments processed by a station in a given time, number of bills of type X processed in a given time, Average time to process a payment, etc.
- ✓ Citizen Experience Attributes:
  1. Same consistent straightforward payment experience for all the Parish’s main payment types.
  2. Allows citizens to enroll in recurring payments as well as set up a one-time scheduled payment.
  3. Offers and manages multiple payment plans. A payment plan can be setup allowing a fee to be paid in installments using an auto-pay function.

4. A shopping cart is used to pay multiple requests in one session.
5. Provides a facility for refunds, credits, charge backs, and voids. A citizen may cancel an electronic payment prior to-designated cut-off.
6. Provides multiple approval levels for selected transaction-types.
7. Provides automatic citizen notifications
   - An email/SMS text reminding the citizen of a pending payment
   - An email/SMS test that a stored credit card is about to expire. Notifications can be set at 60 days and 30 days prior.
   - An email /SMS text that the payment was made with a link to the transaction receipt.
   - An email/SMS text if the payment is rejected.
8. Offers a host of citizen self-service features including:
   - An enrolled user can have access to payment history across all payment types
   - Display current and past bills with the option to download in a pdf format.
   - Citizens maintain their own account profile with full access to payment history and outstanding bills.
   - Scheduling a one-time future payment on the date the citizen prefers using MasterCard, Visa, Discover, American Express or eChecks.
   - Schedule recurring payments using MasterCard, Visa, Discover, American Express or eChecks.
   - Download payment history in pdf or csv formats.
   - Online management of citizen profile information.
   - Set-up and manage payment plans and schedule future payments with automatic ACH or card payments.
   - Store credit card tokens allowing the use of a stored credit card number for future payments
   - Schedule one-time payments
   - Setup recurring payments
   - Manage passwords
   - Manage email addresses

✓ <u>Versatility Attributes:</u>

1. Card processor agnostic, allowing the Parish to work with the gateway service provider of the Parish's choice.
2. Provides the ability to handle multiple fund accounting.
3. Does not place limits or restrictions on the number of items to be paid in one transaction.
4. Allows the user to attach images to a transaction from a local drive or network share.
5. Payment types available include:
   a. One-time payments
   b. Scheduled payments
   c. Automatic Payments
   d. Payment Plans
6. Provides the ability to handle credit or debit card transactions (regardless of

card reading device manufacturer or model) including:

a. Reading and decoding magnetic strips
b. Works with EMV chip technology
c. PIN Pads
d. Keyboard entry
e. Authorization through an online third-party processor/Gateway
f. Receipt printing for credit/debit transactions
g. Digital signature capture
h. Reporting on all credit/debit transactions

✓ Configurability Attributes:

1. Configurable workflow with no programming necessary.
2. Configurable by designated Parish staff to include at a minimum:
   a. User creation/security and/or integration with Active Directory
   b. Customizing/creating reports/ad-hoc
   c. Customizing/creating receipts
   d. Add, edit, and delete data from rate/fee tables
   e. Add, edit, and delete data from fund tables
   f. Change system settings (security, paths, protocols, services, resources)
3. Manage, Create and Edit settings using *Quick* Payments point-and-click system templates:
   a. Define user roles and allowed functionality.
   b. Define receipt and email templates by application or transaction type.
   c. Define transaction approval thresholds.
   d. Define payment options by application or transaction type.
   e. Full Web branding
   f. Secure role-based access to all system functions with support for active directory.
   g. Email, text, and invoice templates are customized using Microsoft Word templates.

✓ Accounting Reconciliation Attributes:

1. Provides automatic merchant services statement reconciliation.
2. Provides automated bank statement reconciliation.
3. Multiple general ledger entries can be generated for all payments when they are posted and when they are reconciled. These automatic ledger entries can significantly speed up the backend accounting process.
4. Includes automatic reconciliation features to streamline the reconciliation process by automatically matching bank and merchant statements to payments made. These automated tools can speed up the reconciliation process for backend accounting staff. An overnight process automatically reconciles banking and merchant services statements with payments made. When the accounting staff signs in to start their day, matched transactions are on the reconciled report and any non-matches are queued for research. This unique feature can streamline the accounting and accounts payable processes allowing staff to concentrate on problem transactions.

5. Provides a full-service eBilling feature set, to include:
    a. A citizen can register for eBilling within citizen self-service. Enrollment is confirmed via email and SMS text.
    b. Email and SMS text statement delivery – A billing file is received from the host and email statements are created and emailed to citizens. A link to the PDF that requires authentication before downloading.
    c. Email and SMS text of past due notices.
    d. Email and SMS text of the Parish correspondence to a single citizen, a group of citizens or all citizens.
    e. Email and SMS text notification of an upcoming automatic payment and when an automatic payment has been processed.
    f. Email and SMS text notification of status in the *Quick* Payments Approval Workflow for refunds and credits:
        - Approval is pending
        - Approval is given or denied.

✓ <u>Other Attributes:</u>

1. Compatible with third party payments options such as PayPal®, Apple Pay®, Google Pay® and others.
2. International debit and credit cards are acceptable with settlement in US Dollars.
3. Screens are customized to provide the look-and-feel of the Parish system.
4. Creates a real-time electronic receipt that is displayed on the screen, sent via email and/or SMS Text, and can be downloaded in PDF format for printing. PHI data is not included on the receipt.
5. Supports unique business rules and receipt formats for each individual payment type.
6. A shopping cart feature allows payment of multiple invoices with a single payment request in one session.
7. Payment can be made up of one or more payment options:
    - Credit Cards – MasterCard, Visa, Discover, American Express
    - Debit cards – MasterCard, Visa
    - Electronic ACH Checks
    - Digital Wallet
8. All card transactions are authorized in real-time.
9. Convenience fees (if any) are added to the receipt as a separate line item.
10. Citizen Self-Service features allow citizens to maintain their own account profile with full access to payment history and outstanding bills.
11. Stores credit card tokens allowing the use of a stored credit card number for future payments
    - Schedule one-time payments
    - Setup recurring payments
    - Manage passwords
    - Manage email addresses

12. A citizen can research and view their payment history across all departments where payments have been made. The citizen can download or email payment history in a variety of file formats including PDF, CSV, MS Word, and MS Excel.
13. Electronic billing features delivering bills to citizens via email.
14. Citizen Self-Service features allow citizens to maintain their own account profile with full access to payment history and outstanding bills.

A. The Citizen Experience

Fairfax Software designed *Quick* Payments with a focus on the citizen experience. Listening to our citizens and *their* citizens has helped us continuously improve the citizen experience.

Consistent User Experience

Quick Payments will provide a consistent experience across all the Parish *Quick* Payments screens.

- **Parish Branding** - Using point and click setup, screens are branded for each business unit setup within *Quick* Payments allowing each business unit to have their own web branding to match the look-and-feel of their current website. This design gives citizens the confidence their payment is being processed by the Parish. Branding extends beyond the website to receipts, invoices, emails, and other communications.
- **Pay as a Guest** – Citizens can make a payment as a guest without registering with the system. This feature can be enabled or disabled by business unit and payment type. For example, a guest payer can pay for a parking permit while a property tax payment requires registration.
- **Ease of *Quick* Payments Registration** – Our secure account registration process is very familiar and new users will feel comfortable with the process.
- **Citizen Dashboard** – When a citizen logs in the first screen displayed, the Citizen Dashboard gives them a quick look into their account history automatically. The dashboard will save time and provide information without having to process a request.

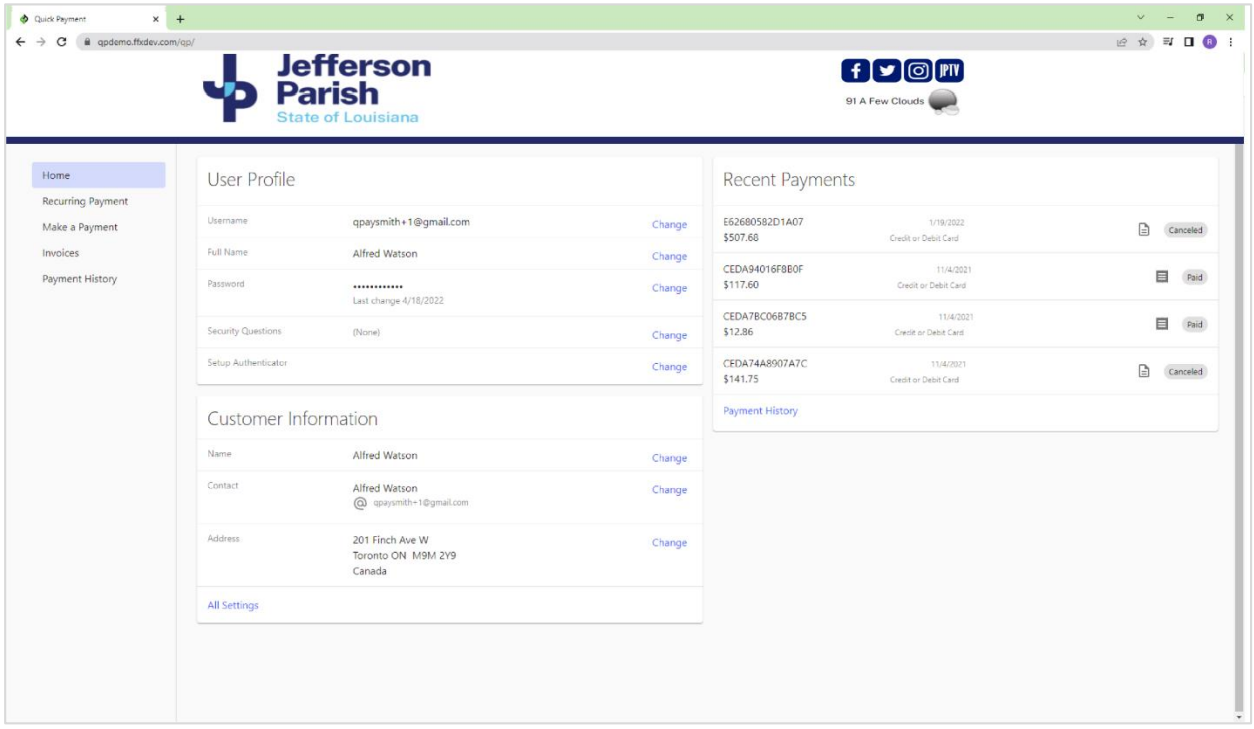


Figure 3 – Citizen Dashboard

- **Recurring Payments –** If allowed by the business unit, a citizen has the option of setting up recurring payments in several different ways:
    - Automatically pay the amount due when a new bill is received
    - Recurring payments can be set up for payment by ACH or credit card.
    - Setup a payment plan to pay a bill monthly until the bill is paid in full. Based on the Parish business rules for payment plans, the system can:
        - Allow a citizen to set up a payment plan without an approval
        - Allow a citizen to set up a payment plan that is submitted to an approval workflow that requires the Parish administrator approval before the plan goes into effect.
        - Allow a Parish Administrator to set up a payment plan on behalf of a citizen.

- **Search for Bills** – A citizen has many options when searching for bills. A table of bills displays based on the search parameters. The local *Quick* Payments SQL database is searched as well as the AS400 system for any new bills.

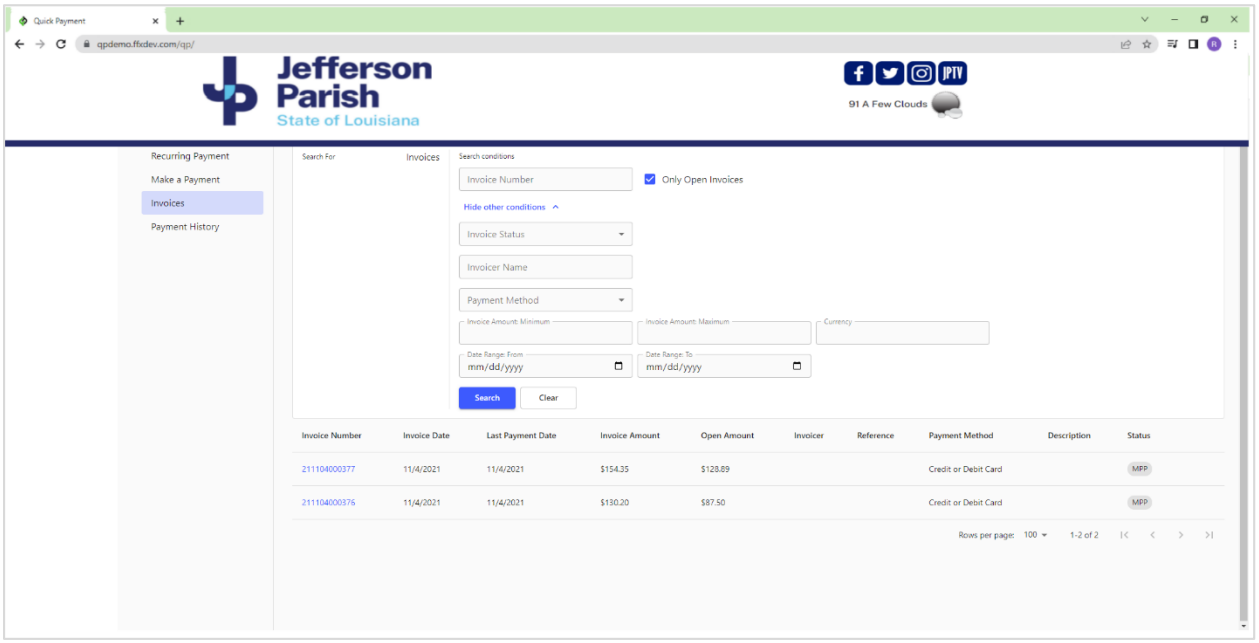


Figure 4 – Research Bills

- **Payment History** – This button will provide a complete payment history for the citizen. The local *Quick* Payments SQL database is searched as well as the AS400 system to list any payments recorded outside of *Quick* Payments.

  A link to the receipt and bill for each payment is provided for display on the screen. Receipts and bills can be downloaded to the local machine in a variety of formats including PDF, MS Word, MS Excel, and CSV.

- **Make a payment** – Payments are initiated by looking up a bill or selecting a service and selecting the pay button. Payment options, subject to Parish business rules, include:
  - **Credit or Debit Card** – pay with one or more credit or debit cards
  - **eCheck** – pay by one or more ACH transactions
  - **Scheduled Payment** – process the payment at a future date
  - **Monthly Payments** – set up a payment plan

B. The Parish Business Administrator

A Parish Business Administrator will have their own view in the admin portal. Features of the portal are turned 'on' and 'off' based on the login role of the user. Business Administrators can be restricted to their business unit or have access to multiple business units. For example, a business administrator at the Animal Shelter has access to all transactions for the Animal Shelter but does not

have access to other business units. A more senior administrator may have access to all Parish transactions. Roles are defined for each type of administrator to restrict access as required by Parish security requirements.

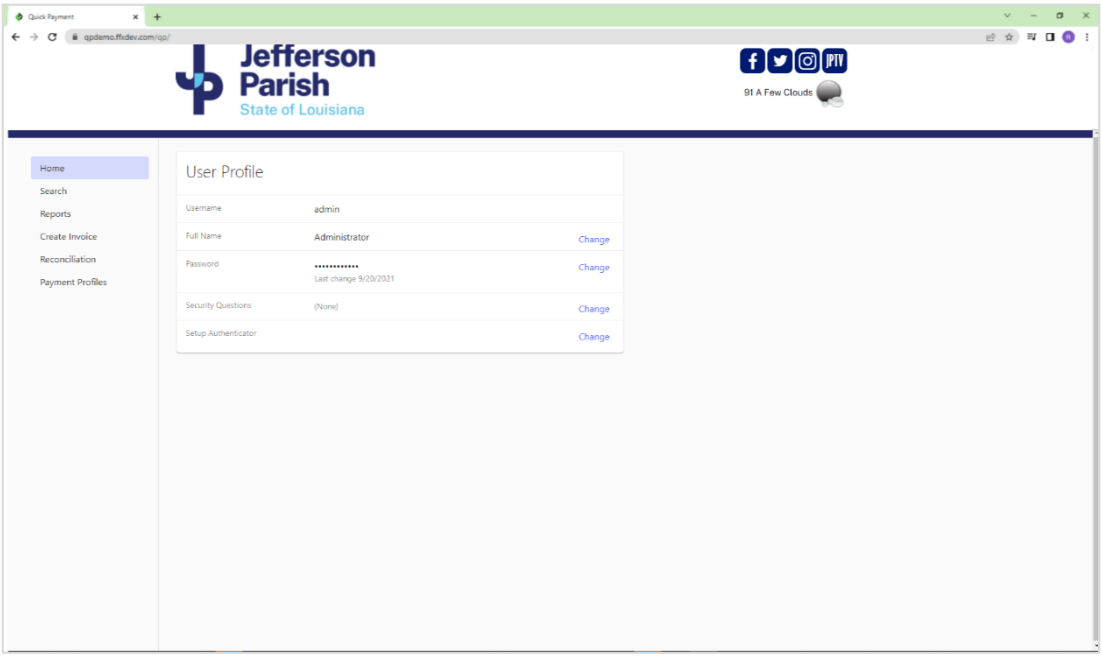


Figure 5 – Business Administrator Home Screen

- **Search** – Research Bills/Invoices, Auto Pay History, Credit Memos, Past Due Notices, Payment History. Research can be limited to a specific date, range of dates, bill/invoice status, name, account number, payment type, or transaction ID. Any combination of search criteria can be used to retrieve the desired results.

  A list is returned matching the search criteria. From the list, the user has a link to a view a PDF of the bill/invoice, add comments, initiate a refund or credit memo, setup a payment plan, download a spreadsheet that contains the details returned in the pick list or download the details of a single bill/invoice.

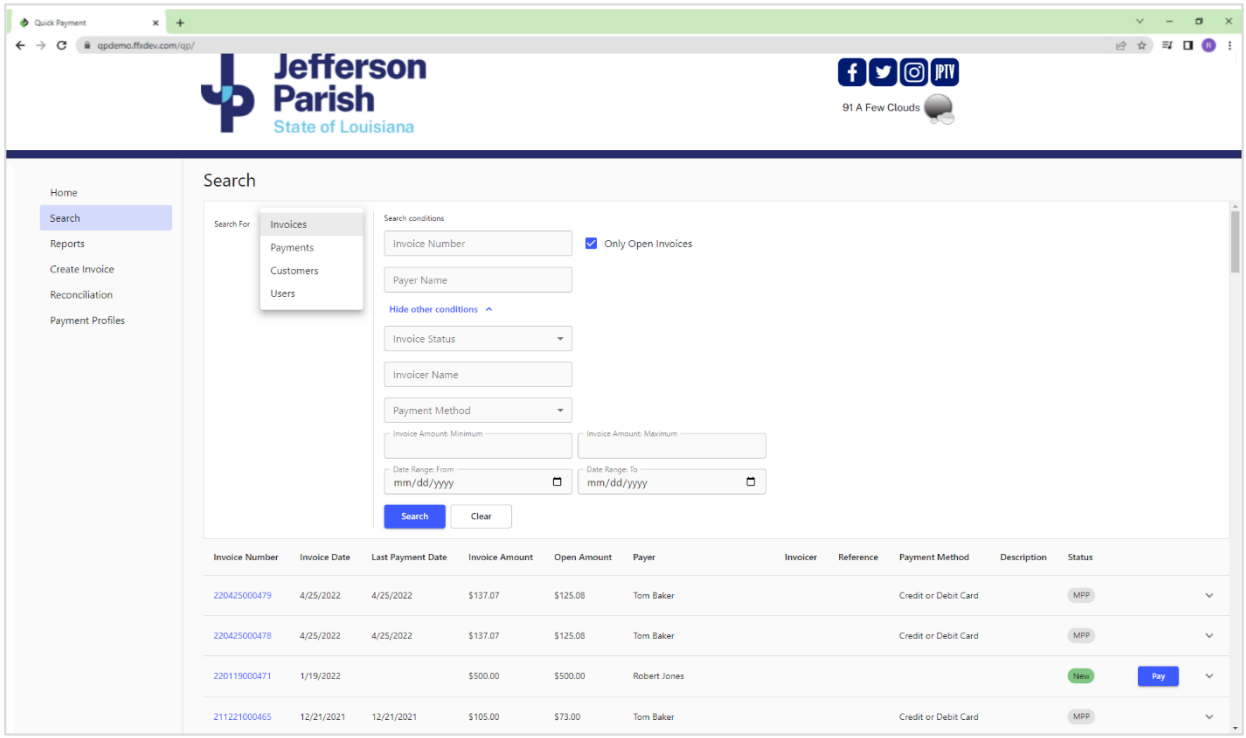


Figure 6 – Business Administrator Search Screen

- **Account Reconciliation** – Access to the results of automatic statement reconciliation of bank accounts and merchant provider accounts. A daily reconciliation file is open until all contents of the file have been matched to corresponding payments. This is a tool that streamlines the work of the accounting department. Each business unit can reconcile their own merchant accounts or reconciliation can be centralized.
- **Reports** – View automatically generated reports as well as create ad-hoc reports. Reports can be run on a specific date or range of dates. Reports can be viewed or downloaded in a variety of formats including PDF, Word, and Excel. the Parish has control over all system reports. Standard reports include:

  Accounts in Collections
  Aged Receivables Report
  Audit Events
  Collections Report
  Credit Memos applied to Open Invoices
  Credit Memo Raised
  Delinquent Accounts
  Deposit Reports
  Overpayments
  Revenue Received
  Revenue Report
  Underpayments
  Underpayments and Overpayments

- **Raise a Credit Memo** – The user can raise a Credit Memo against a payment that has been already made - The user must provide notes explaining the request. A credit memo must be raised by an internal Parish user on behalf of a citizen.
- **Request a Refund** - The user must provide notes explaining the request. A refund request must be raised by an internal Parish user on behalf of a citizen. Default business rules prevent a citizen from requesting a credit note within the citizen self-service feature of the application.
- **Approval Workflow** – A credit note, or refund request is added to an approval queue. An administrator can be authorized to approve a refund or credit note up to a certain dollar value; For example, a team lead can approve a request up to $1000 but $1001 or above must be approved by a manager. Up to 5 different delegation levels can be set up in the workflow. If a refund or credit note is requested by a user that has approval status, they cannot approve their own request. Another administrator must approve the request.

  When a request is made, the citizen receives a notification that the request was made and is pending approval. The request is automatically added to the approval workflow queue. The queue is accessible to all users with approval authority for the specific request. A number is displayed indicating the count of approvals that are pending. The approver can view the request and the notes provided by the requestor. The approver then accepts or denies the request. Notes explaining the decision are required.

  The citizen receives a notification that the request is granted or denied along with the notes provided by the reviewer. Each step of the process is included in the system audit.

C. System Administrator

A Parish System Administrator view into the portal allows the Parish technical staff to maintain the system. Different administrator roles can be established to restrict functions to specific users. For example, only a security administrator role has the ability to add, modify, and delete users.

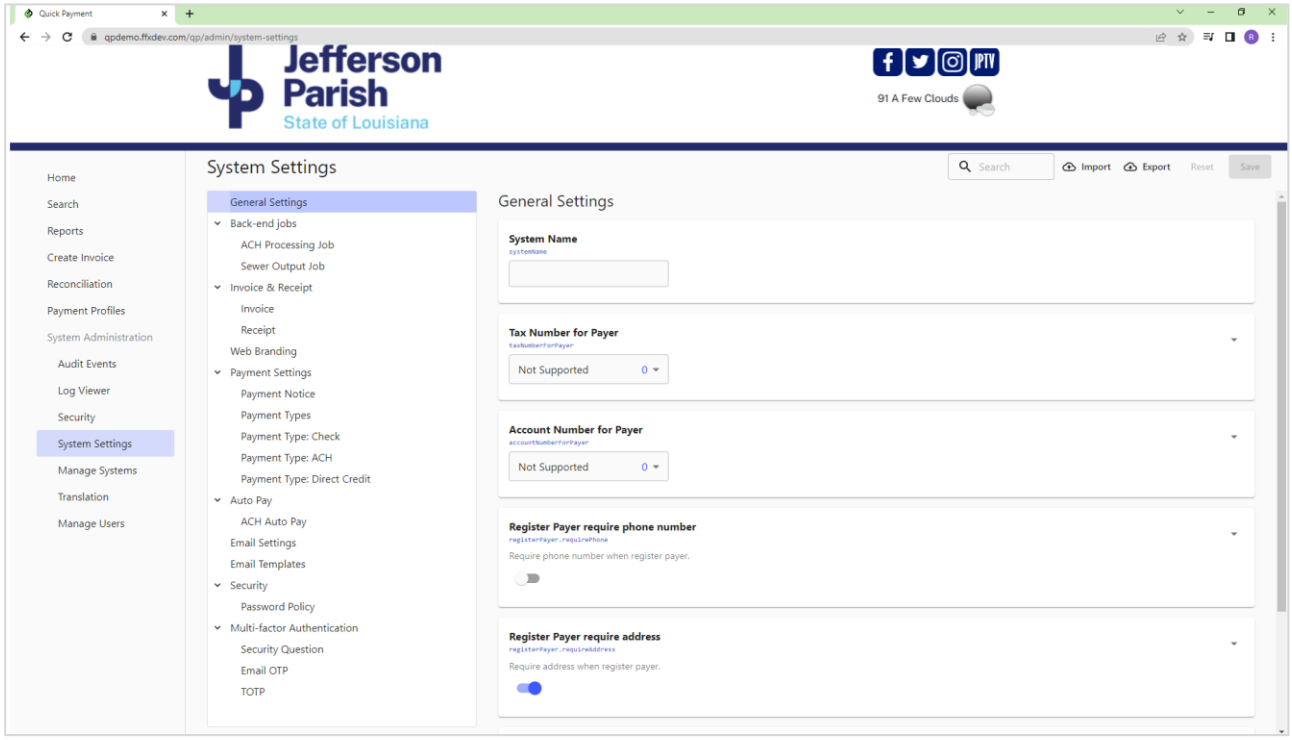


Figure 7 – System Administrator View

- **Audit Events** – the Parish technical Staff can view and download audit information stored in the audit database.
- **Log Viewer** – the Parish technical staff can view, research, and download system logs.
- **Security Settings** – the Parish security administrators can add, modify, and assign roles and privileges for different user groups accessing the system
- **Manage Users**
  - **Add, Modify, Delete Internal the Parish Users –** Internal users are created in the system by an administrator that assigns the user to the role or roles that control the user's access. This feature should be restricted to a separate security administrator at the department or the Parish level.
  - **Add, Modify, Delete Public Users –** This feature allows a Department Administrator to assist a citizen to create a user account on their behalf. The citizen will complete registration by setting their own password and authentication credentials.
- **System Settings –** This feature allows the Parish technical and business staff to set system templates that establish business rules and processing options that control how *Quick* Payments operates. These point-and-click system templates do not require application programming.

- Security Parameters - Set password policy and multifactor authentication parameters.
- Schedules – Set schedules for system activities like receiving files, billing runs, receiving statement files etc.
- Notifications – Define email and text notification content.
- Receipt Templates – Microsoft Word templates are used to define the format for the receipt generated when a payment is received.
- Web Branding – Set header, footer, and website Custom Style Sheets (CSS) files to brand *Quick* Payments with the Parish look-and-feel.
- Payment Parameters – Select which payment methods are allowed for a transaction type. All settings for the merchant services provider are included here.
- Auto Pay Settings – Select global auto pay settings for recurring credit card and ACH payments.
- Translator Settings – Access to the translation table used to translate *Quick* Payments screens from English to Spanish and other languages. This allows the administrator to modify the translation provided if needed.

Quick Payments Access Methods

- **Parish Internal User Direct Access**
  Internal Parish users with appropriate privileges will have the ability to log into *Quick* Payments directly.
- **Citizen Direct Access**
  Citizens are able to register with the system and login directly to manage their own user profile. Citizens also have access to their payment history. At the Parish's option, access can be set up to require a citizen to access *Quick* Payments only through a link provided by the Parish application.
- **Access to *Quick* Payments by a Redirect Link**
  Citizens can select a link within the Parish application to initiate a payment. When redirected to the Parish's *Quick* Payments website, the citizen will have an option to login to *Quick* Payments if they are a returning user or register with the system if they are a new user. The citizen can also pay as a guest without registering with the *Quick* Payments system. Registered citizens can access all citizen self-service features of the system.

Quick Payments Workflow:

A. **Make a Payment Online -** A citizen downloads and pays a bill generated by the business unit. For example, a utility bill generated by the AS400.

A citizen logs into *Quick* Payments to make a payment. Integration with the backend system will allow the citizen to download outstanding bills, view them on the screen exactly as they were created by the backend system, and pay electronically.

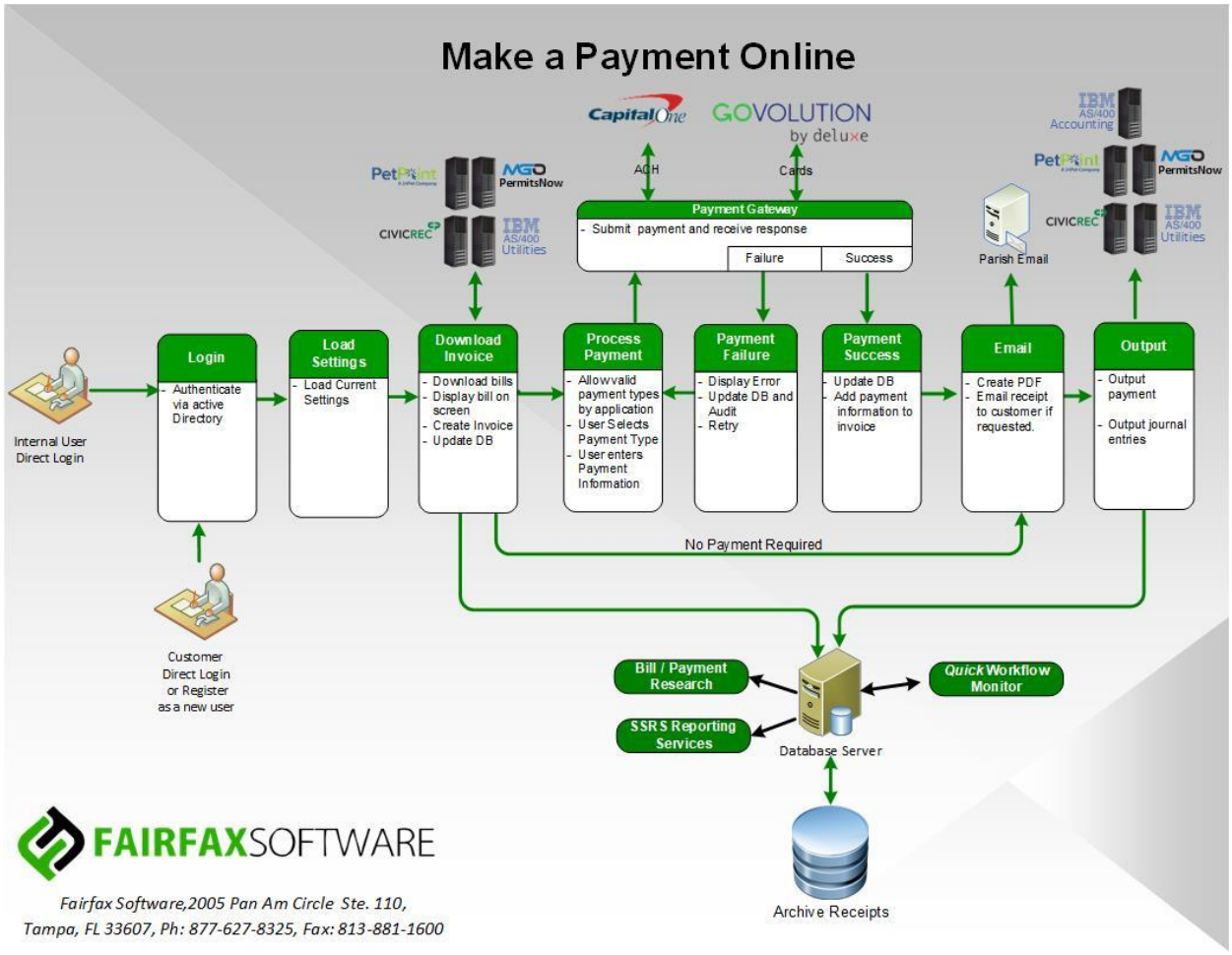


Figure 8 – Make an Online Payment – Billing System Generates the Bill

Transaction Workflow

1. Login – The citizen can login to *Quick* Payments as a returning citizen or register as a new citizen.
    - The citizen can be redirected to the login page from the Parish application or at the Parish's option, the citizen can be allowed to access the page directly.
    - A Parish internal user can login and be authenticated by Active Directory.
    - An internal user must be added by the Parish Systems Administrator
2. Load Settings – *Quick* Payments will load current application settings.

3. Retrieve bill – *Quick* Payments will search for outstanding bills due for the citizen to view and pay. Outstanding utility bills are retrieved from the AS400 system. For example, John Smith logs in to pay a bill. *Quick* Payments will search the billing system for outstanding bills for John Smith or the requested billing address. All the utility bills matching the search are returned.

   Quick Payments can ingest a daily billing file from the AS400 or via web-services API's, bills can be looked up in real time.

4. The user selects a payment option that is valid for the application. More than one payment option can be selected.
5. Payment Gateway - the payment request is sent to Govolution for processing Credit Cards, Debit Cards, or digital wallet transactions. All credit card information is directly entered into Govolution. No PCI data is stored in the *Quick* Payments system. ACH Checks go to the Parish designated bank, Capitol One.
6. Payment Failure - The payment was denied by merchant services provider. The return codes and messages are added to the receipt and written to the database. The user has the option to try again.
7. Payment Success - the transaction ID and confirmation codes from the gateway are added to the receipt and recorded in the database. A token representing the transaction is stored in the database. No credit card information is saved in the *Quick* Payments SQL database.
8. Email - Receipts are generated in PDF format and automatically emailed and/or texted to the citizen.
9. Output - The payment is marked in the database to be included in the day's posting file for and journal entries are created to update the Parish accounting system.

B. **Voids, Refunds and Credit Notes: An** internal user can initiate a void, refund, or credit note for a transaction that was previously completed. The Parish has the option to require an approval by an administrator before refunds or credit notes are granted.

- Voids - A transaction can be voided by an internal administrator before payment is settled at the end of the day.
- Refunds – A transaction can be refunded after payment has been settled.
- Credit Notes – A Credit Note is created when the original payment method cannot accept a refund. For example, the credit card account used for payment has since been closed.

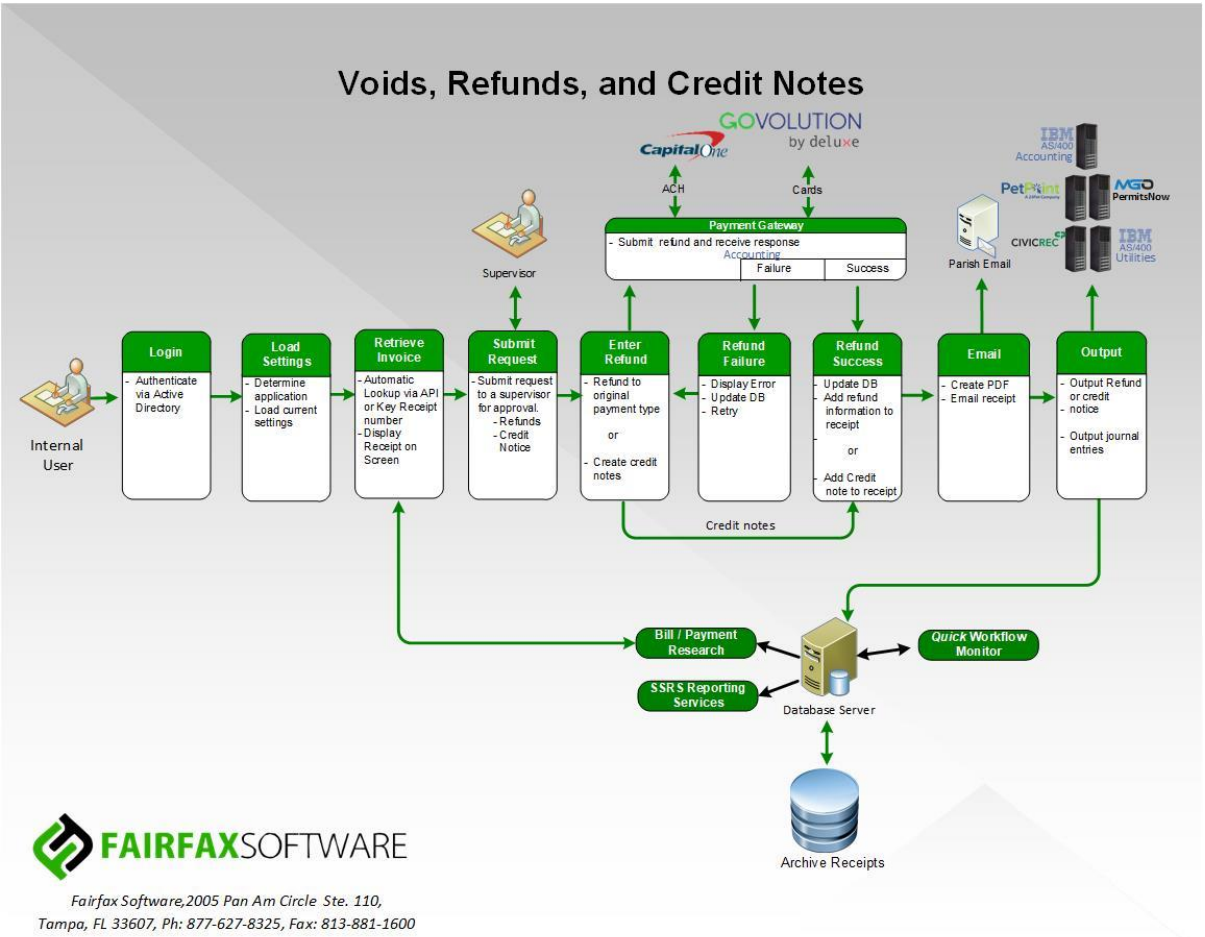


Figure 9 – Refunds and Credit Notes

Transaction Workflow

1. Internal User Login - An internal user logs directly into *Quick* Payments and is authenticated. Voids, refunds and credit notes are initiated by internal users.
2. Load Settings - *Quick* Payments will load current application settings
3. Receipt - The user retrieves the payment receipt from the payment archive.
4. The system displays the receipt on the screen for the user to review. This is the receipt where the void, refund or credit notice, will be created against.
5. Submit a Request - The user enters the required information to request a void, refund, or a credit note. A reason code is required.
    a. A Void is issued prior to settlement of the original funds
    b. A Refund credits the citizen's account via the original payment method.

c. A Credit Note is issued when the original payment method is no longer available or does not accept refunds. The system will track credit notes allowing the citizen to use them as payment for a future transaction.

   If the Parish reimburses the citizen, a Credit Note can be cleared by a Parish Administrator. For example, the Parish cuts a check to reimburse the citizen using a process outside of the *Quick* Payments system.

6. Void – Debit and credit card voids are processed by the Parish credit card clearing provider and through the proposed system. Payment is voided and removed from the settlement file. The transaction does not appear on the citizen's credit card statement.
7. Refund - Debit and credit card refunds are processed by merchant services provider. Credit Notes bypass the payment gateway.
8. Refund Failure – Merchant services provider has denied the refund. The denial code and explanation are displayed on the screen and recorded in the database. The user has the option to try again or cancel the transaction. For example, a credit card refund cannot be refunded because the account is now closed.
9. Refund Success - The refund has been approved. The receipt is updated with the transaction information and approval codes and recorded in the database.
10. For approved credit notes, the receipt is updated with the transaction information and approval codes and recorded in the database. The citizen can now use the credit note against a future payment.
11. Email - Receipts are generated in PDF format and automatically emailed to the citizen.
12. Output - Refunds and credit notes are marked in the database to be included in the day's posting file and journal entries recreated for the accounting system.

C. Integrated Voice Response (IVR) Payment Processing interfaces with *Quick* Payments via secured web services APIs. All payments are processed through *Quick* Payments using the same business rules and are processed together with other online payments.

Advanced IVR solution

Allows callers to lookup one or more bills/invoices and have the IVR solution present the associated bill amounts and bill due dates. The caller then is afforded the option to select all overdue bills for payment, overdue and current bills for payment, or future bills for payment. Payments can be made via credit card or online check.

Our IVR solution can be set up to assess a convenience/service fee. Our IVR solution can offer multiple languages, as needed. Additionally, our IVR solution can be configured to support multiple payment types (i.e., press 1 to pay your real estate tax, press 2 to pay your utility bill, etc.). The payer can also zero out to a particular Agency as needed.

Once the citizen calls into the toll-free number provided, they can look-up their bill with an identifier that the Parish requires. The citizen will then receive the amount, due date and any other related voice activity requested by the Parish. The payer can then make their payment using a card or electronic check. The IVR then provides a confirmation number that the citizen and Parish can reference back to the host system. In addition, the citizen has the option to receive a text notification of the payment. If the citizen is a repeat payer on the IVR system, they can also choose to save their payment information for later use the next time they access the IVR system.

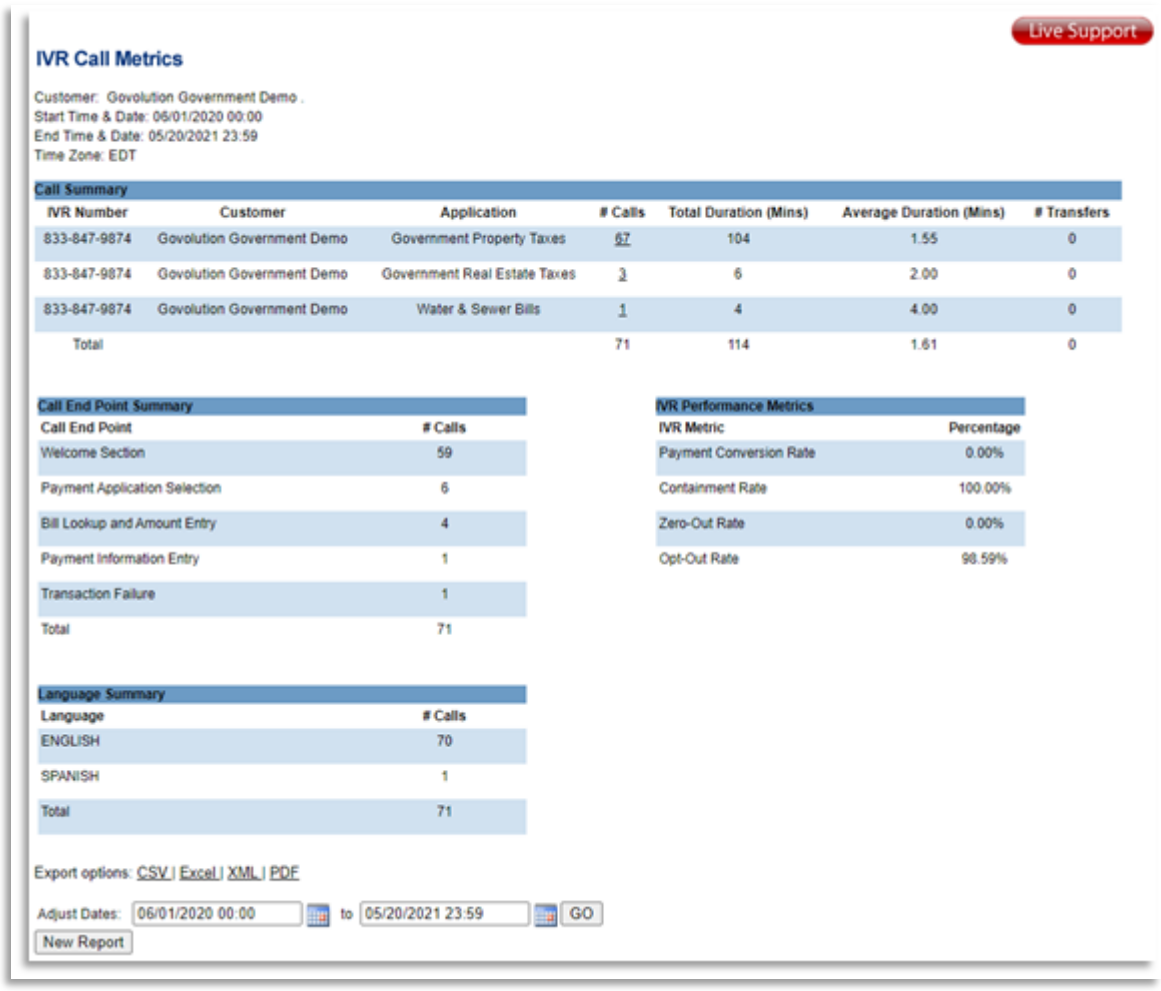
IVR call metrics are provided, where the Parish can view details of all payments being made through the IVR. The Parish can see things like minutes, number of calls per language, call endpoint that gives the Parish eyes on where users are abandoning their call so that improvements can be made in the call flow if needed.

- Call Summary
  - IVR Number
  - Customer
  - Application
  - Calls
  - Total Duration of Call
  - Average Duration of Calls
  - Transfers

- Call End Point Summary
  - Welcome Section
  - Payment Applications Selection
  - Bill Lookup and Amount Entry
  - Payment Information Entry
  - Transaction Failure

- IVR Performance Metrics
  - Payment Conversion Rate
  - Containment Rate
  - Zero-Out Rate
  - Opt-Out Rate

- Language Summary
  - English
  - Spanish
  - Additional languages available upon request



Live Support

IVR Call Metrics

Customer: Govolution Government Demo .
Start Time & Date: 06/01/2020 00:00
End Time & Date: 05/20/2021 23:59
Time Zone: EDT

Call Summary

IVR Number	Customer	Application	# Calls	Total Duration (Mins)	Average Duration (Mins)	# Transfers
833-847-9874	Govolution Government Demo	Government Property Taxes	67	104	1.55	0
833-847-9874	Govolution Government Demo	Government Real Estate Taxes	3	6	2.00	0
833-847-9874	Govolution Government Demo	Water & Sewer Bills	1	4	4.00	0
Total			71	114	1.61	0

Call End Point Summary

Call End Point	# Calls
Welcome Section	59
Payment Application Selection	6
Bill Lookup and Amount Entry	4
Payment Information Entry	1
Transaction Failure	1
Total	71

IVR Performance Metrics

IVR Metric	Percentage
Payment Conversion Rate	0.00%
Containment Rate	100.00%
Zero-Out Rate	0.00%
Opt-Out Rate	98.59%

Language Summary

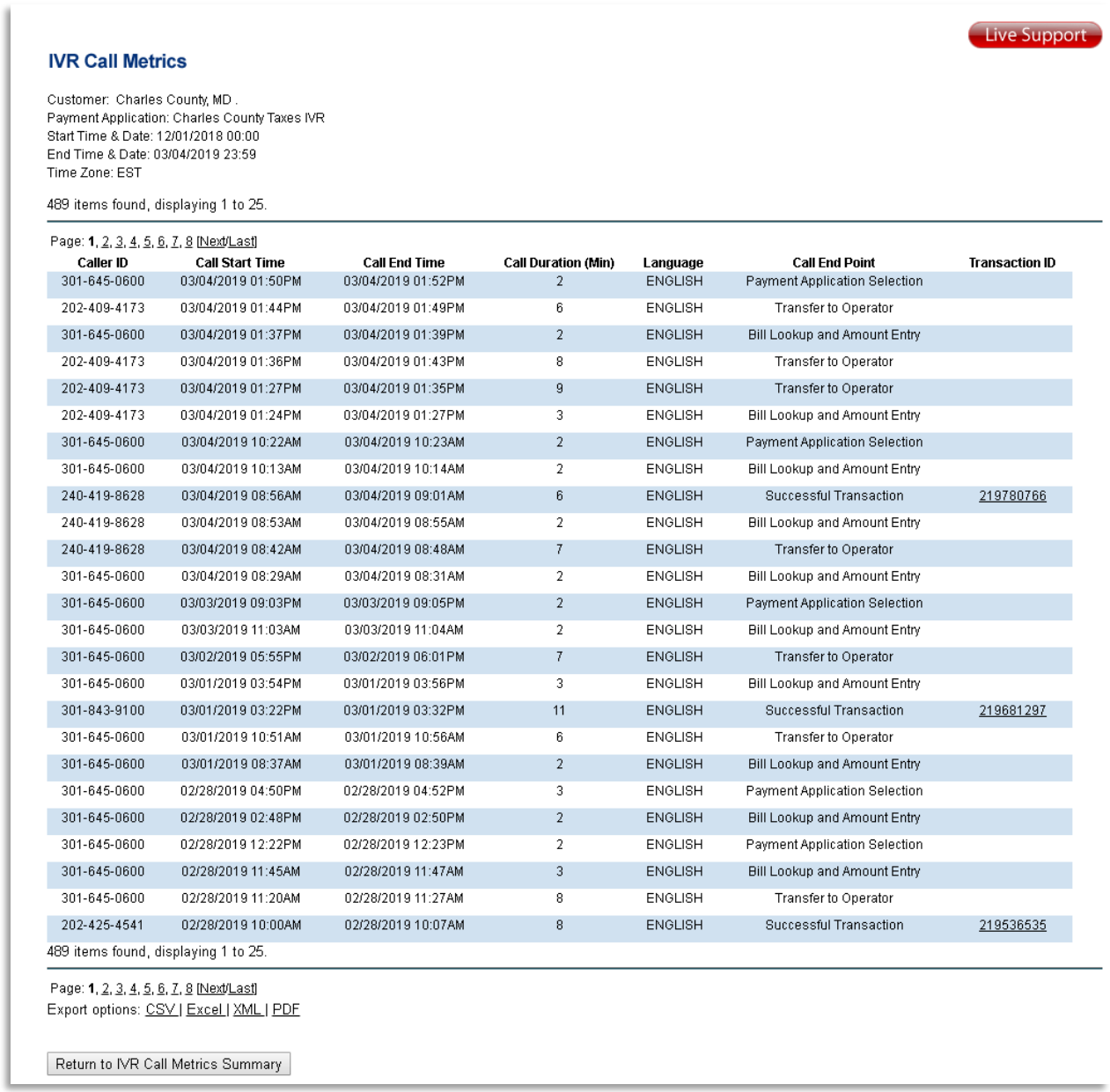
Language	# Calls
ENGLISH	70
SPANISH	1
Total	71

Export options: CSV | Excel | XML | PDF

Adjust Dates: 06/01/2020 00:00 to 05/20/2021 23:59 GO

New Report

Figure 10 – Sample IVR Call Metrics



Live Support

IVR Call Metrics

Customer: Charles County, MD .
Payment Application: Charles County Taxes IVR
Start Time & Date: 12/01/2018 00:00
End Time & Date: 03/04/2019 23:59
Time Zone: EST

489 items found, displaying 1 to 25.

Page: **1**, 2, 3, 4, 5, 6, 7, 8 [Next/Last]

Caller ID	Call Start Time	Call End Time	Call Duration (Min)	Language	Call End Point	Transaction ID
301-645-0600	03/04/2019 01:50PM	03/04/2019 01:52PM	2	ENGLISH	Payment Application Selection	
202-409-4173	03/04/2019 01:44PM	03/04/2019 01:49PM	6	ENGLISH	Transfer to Operator	
301-645-0600	03/04/2019 01:37PM	03/04/2019 01:39PM	2	ENGLISH	Bill Lookup and Amount Entry	
202-409-4173	03/04/2019 01:36PM	03/04/2019 01:43PM	8	ENGLISH	Transfer to Operator	
202-409-4173	03/04/2019 01:27PM	03/04/2019 01:35PM	9	ENGLISH	Transfer to Operator	
202-409-4173	03/04/2019 01:24PM	03/04/2019 01:27PM	3	ENGLISH	Bill Lookup and Amount Entry	
301-645-0600	03/04/2019 10:22AM	03/04/2019 10:23AM	2	ENGLISH	Payment Application Selection	
301-645-0600	03/04/2019 10:13AM	03/04/2019 10:14AM	2	ENGLISH	Bill Lookup and Amount Entry	
240-419-8628	03/04/2019 08:56AM	03/04/2019 09:01AM	6	ENGLISH	Successful Transaction	219780766
240-419-8628	03/04/2019 08:53AM	03/04/2019 08:55AM	2	ENGLISH	Bill Lookup and Amount Entry	
240-419-8628	03/04/2019 08:42AM	03/04/2019 08:48AM	7	ENGLISH	Transfer to Operator	
301-645-0600	03/04/2019 08:29AM	03/04/2019 08:31AM	2	ENGLISH	Bill Lookup and Amount Entry	
301-645-0600	03/03/2019 09:03PM	03/03/2019 09:05PM	2	ENGLISH	Payment Application Selection	
301-645-0600	03/03/2019 11:03AM	03/03/2019 11:04AM	2	ENGLISH	Bill Lookup and Amount Entry	
301-645-0600	03/02/2019 05:55PM	03/02/2019 06:01PM	7	ENGLISH	Transfer to Operator	
301-645-0600	03/01/2019 03:54PM	03/01/2019 03:56PM	3	ENGLISH	Bill Lookup and Amount Entry	
301-843-9100	03/01/2019 03:22PM	03/01/2019 03:32PM	11	ENGLISH	Successful Transaction	219681297
301-645-0600	03/01/2019 10:51AM	03/01/2019 10:56AM	6	ENGLISH	Transfer to Operator	
301-645-0600	03/01/2019 08:37AM	03/01/2019 08:39AM	2	ENGLISH	Bill Lookup and Amount Entry	
301-645-0600	02/28/2019 04:50PM	02/28/2019 04:52PM	3	ENGLISH	Payment Application Selection	
301-645-0600	02/28/2019 02:48PM	02/28/2019 02:50PM	2	ENGLISH	Bill Lookup and Amount Entry	
301-645-0600	02/28/2019 12:22PM	02/28/2019 12:23PM	2	ENGLISH	Payment Application Selection	
301-645-0600	02/28/2019 11:45AM	02/28/2019 11:47AM	3	ENGLISH	Bill Lookup and Amount Entry	
301-645-0600	02/28/2019 11:20AM	02/28/2019 11:27AM	8	ENGLISH	Transfer to Operator	
202-425-4541	02/28/2019 10:00AM	02/28/2019 10:07AM	8	ENGLISH	Successful Transaction	219536535

489 items found, displaying 1 to 25.

Page: **1**, 2, 3, 4, 5, 6, 7, 8 [Next/Last]
Export options: CSV | Excel | XML | PDF

Return to IVR Call Metrics Summary

Figure 11 – Sample IVR Call Metrics

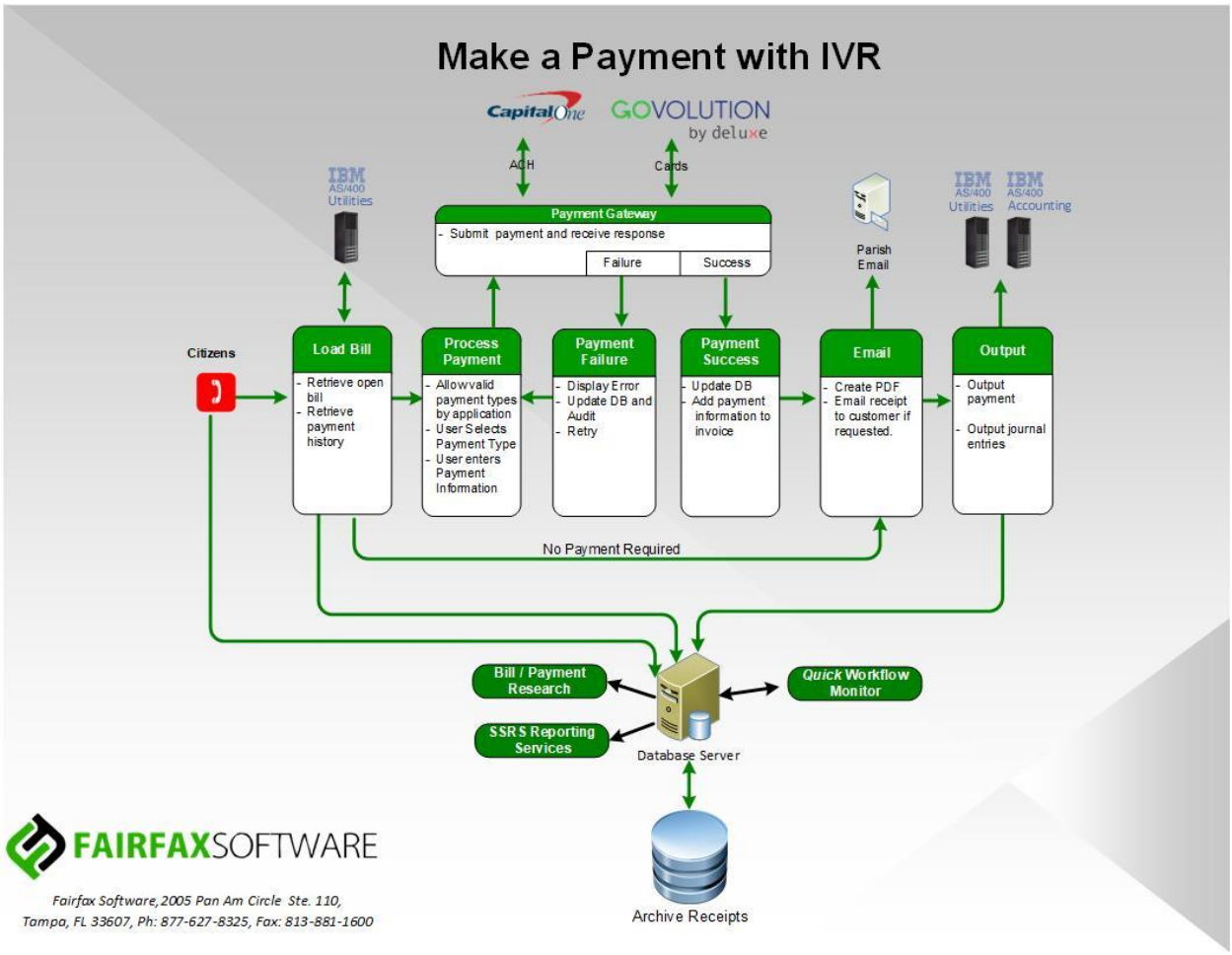


Figure 12 – Pay by IVR

Transaction Workflow

1. The citizen dials the Parish payment phone number.
2. The citizen response indicates English or Spanish preference.
3. Retrieve Bill – the citizen listens to voice prompts that validate the citizen account and requests a bill to be paid. The system retrieves the bill and reads the bill information. The citizen has the option to listen to payment history.
4. The user selects a payment option that is valid for the application and responds to voice prompts to provide required data.
5. Payment Gateway - the payment request is sent to the Payment Gateway for processing. Credit and Debit cards are processed by Govolution and eChecks are processed via ACH to Capitol One. All credit card information is stored directly into the card processing gateway and is not stored in *Quick* Payments or any Parish system.

6. Payment Failure - The payment was denied. The return codes and messages are added to the receipt and written to the database. The user has the option to try again with a different form of payment.
7. Payment Success - the transaction ID and confirmation codes from the gateway are added to the receipt and recorded in the database. A token representing the transaction is stored in the database. No credit card information is saved by *Quick* Payments.
8. Email - Receipts are generated in PDF format and automatically emailed to the citizen.
9. Output - The payment is marked in the database to be included in the day's posting file to AS400 and journal entries are created to update the accounting system.

Quick Payments Screen Shots

A. Paying a Bill Online

Integration via web-based APIs with the backend system allows a citizen to download and pay bills previously generated by the AS400. If a PDF of the bill is not available, billing data is downloaded, and the system will create an invoice that looks like the original bill using MS Word-based templates.

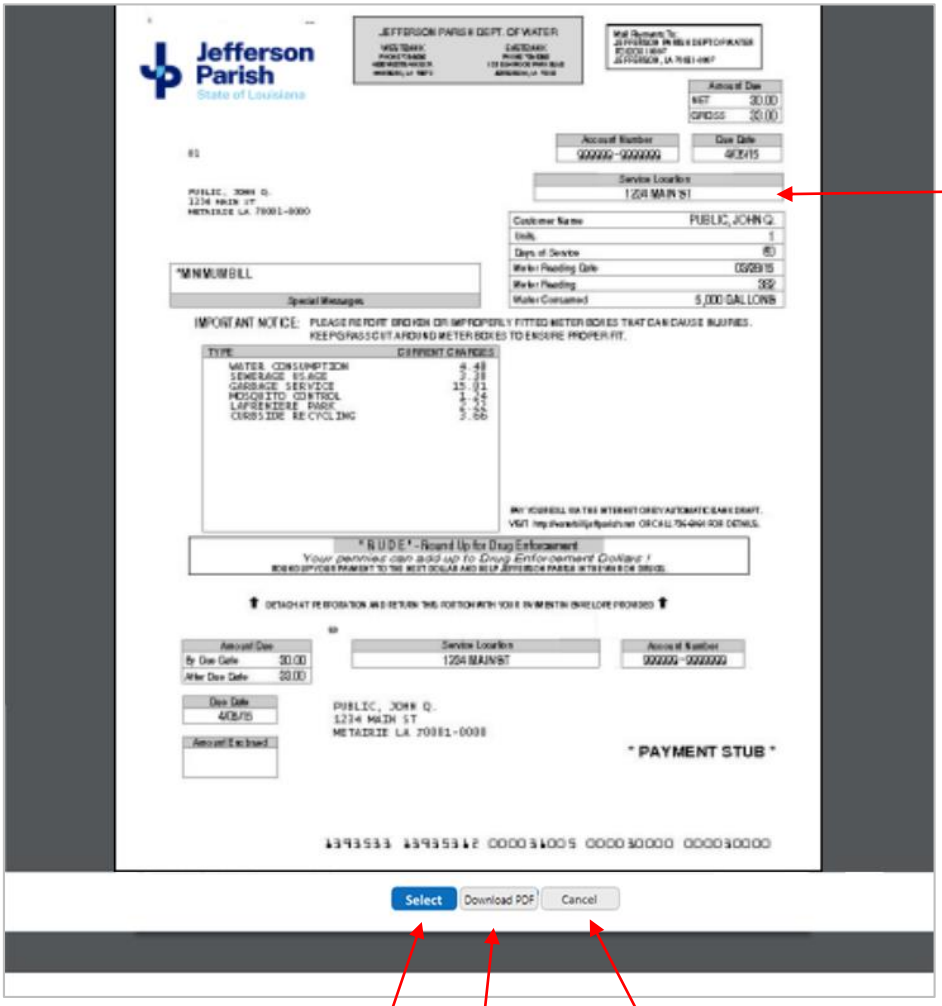


Figure 13 – View Bill

Payment Screen – The citizen has the option to pay the amount or schedule monthly payments

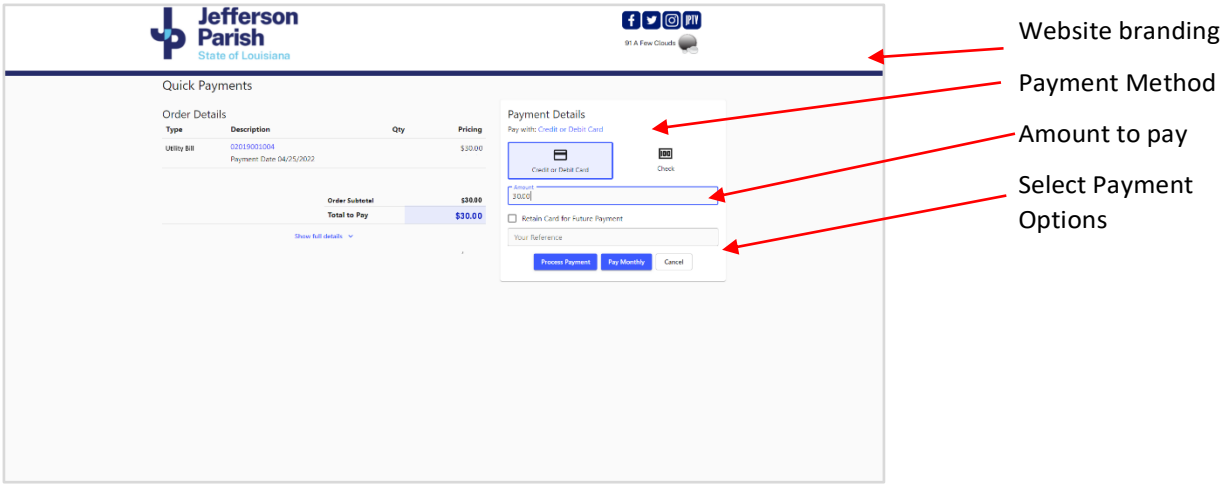


Figure 14 – Payment Screen

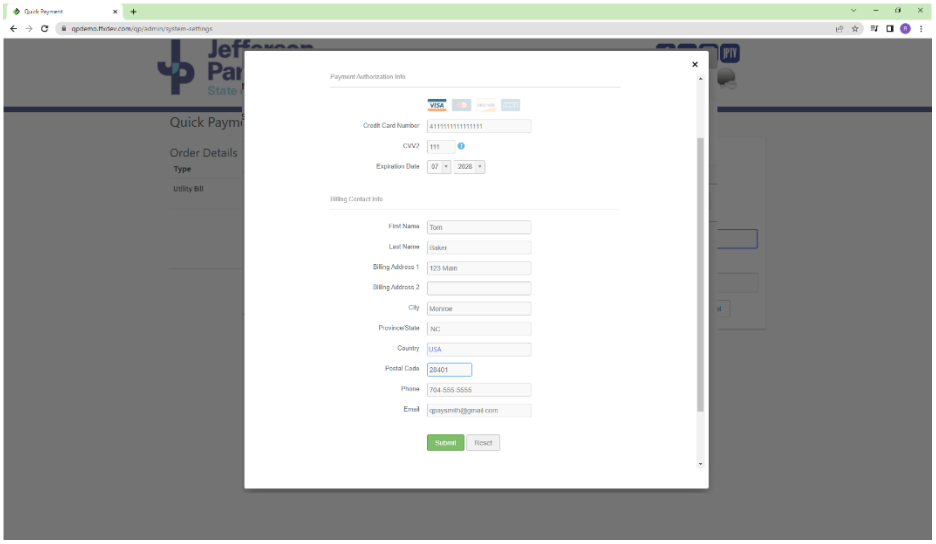


Figure 15 – Enter Card Information

Card information is entered directly into an I-Frame displayed by the credit card gateway. No PCI data is entered directly into *Quick* Payments or stored in the database. The credit card processor returns a token representing the transaction along with the transaction results.

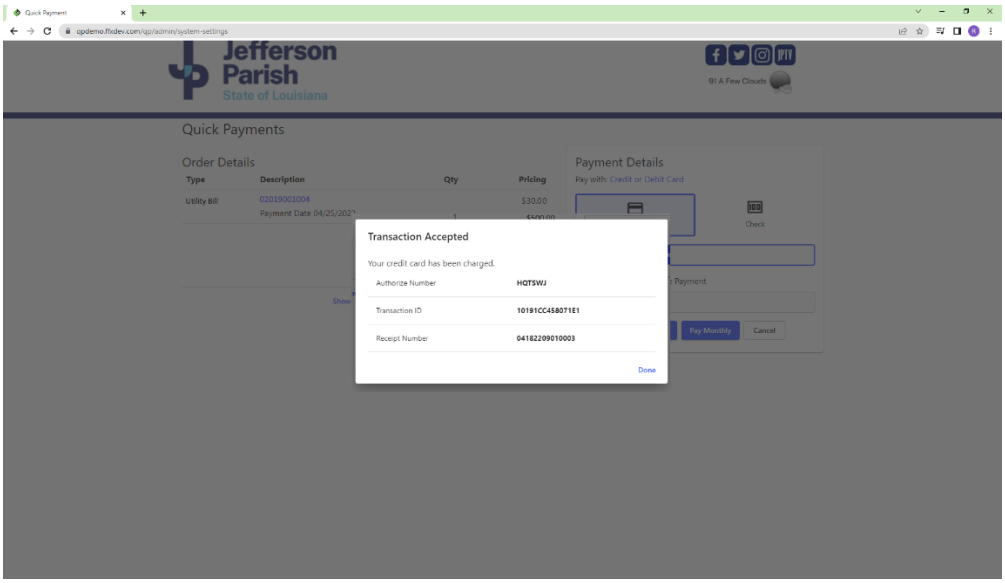


Figure 16 – Transaction Complete

Transaction Receipt

Quick Payments generates a paid receipt as a record of the transaction. The receipt displays on the screen and is automatically sent via SMS Text/Email to the citizen. The citizen has the option to download the receipt for printing. The receipt format is unique to each the Parish application and is set up in the System Template for the application.

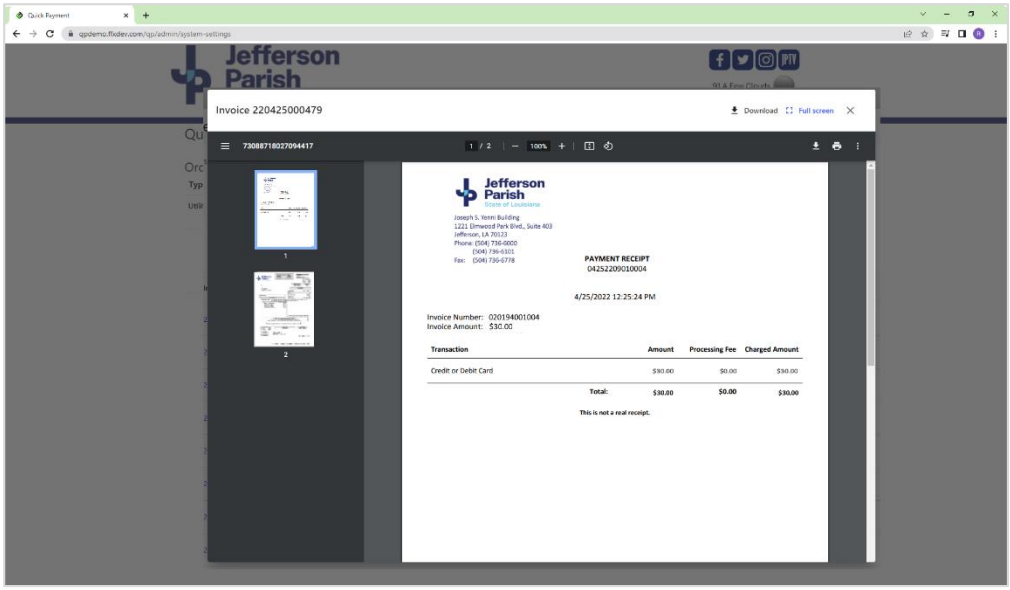


Figure 17 – Transaction Receipt

Email Notification

Quick Payments sends automatic notification for system events. The Parish has control over the content and frequency of notification emails. The following email shows a payment confirmation email. Notifications events include:

- Registration confirmation
- A new bill is now available for viewing and payment (eBills)
- Payment Reminders
- A reminder that a scheduled payment will be processed in 5 days
- Payment confirmation
- A password has been reset

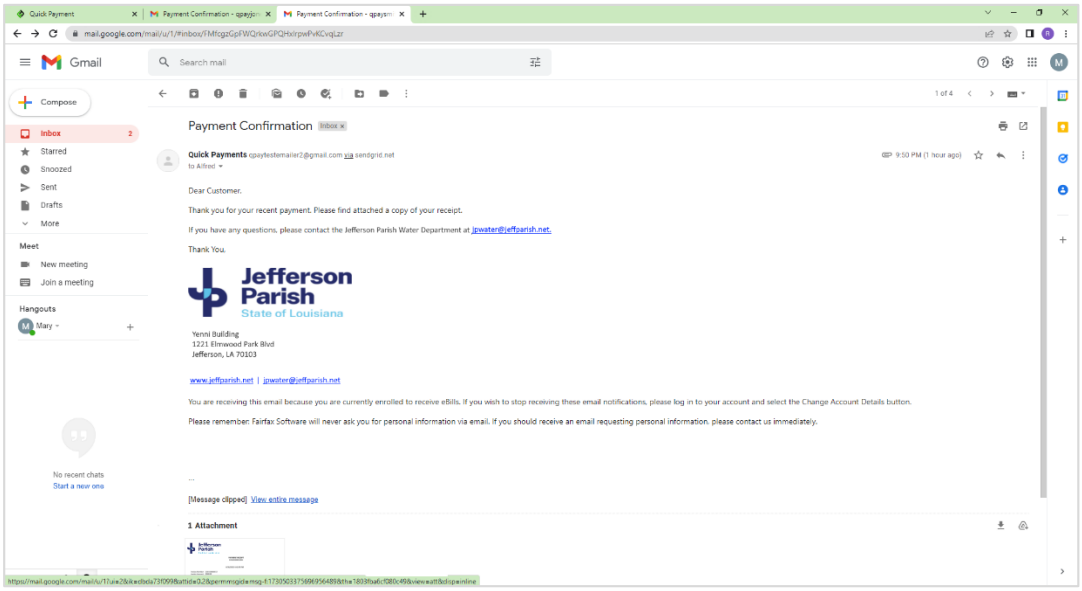


Figure 18 – Email Notification

B. Online Payments with Mobile Devices

Quick Payments is an HTML-5 application designed to process as a hybrid mobile application that runs on any smartphone or tablet that has an internet browser. This includes Apple iOS and Android devices. A hybrid mobile app uses the device's browser to display HTML pages. To the citizen, a hybrid mobile application has the same look and feel of a native application downloaded from the app store.

Using a hybrid mobile application means that any modifications to the *Quick* Payments online portal are instantly available to the mobile application.

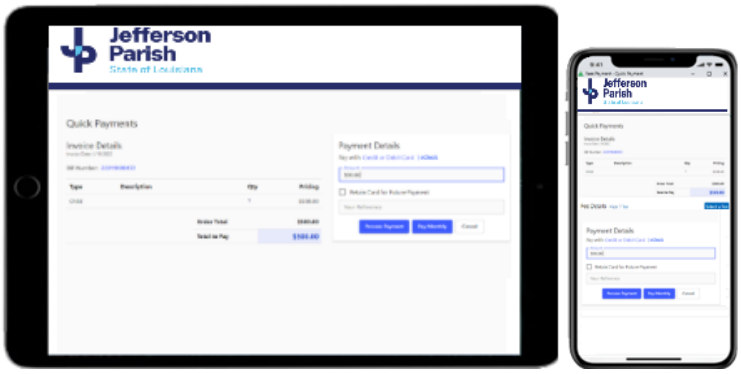


Figure 19 – Tablet and Smartphone Based Payments

Tools Outside the Workflow

A. *Quick* Research

The *Quick* Research web services API is provided to allow the Parish to integrate research functionality into their systems. The user is authenticated to restrict search capability by login privilege. For example, a citizen can only have access to their own transactions where an internal Parish user would be able to research all transactions. The API will allow the user to search the Invoice and Payments database. Results can be displayed on the screen or downloaded in a CSV or PDF format. Research capability is also provided in the *Quick* Payments application. Research fields include:

- Receipt number
- Citizen name
- Entity name
- Entity reference
- Case reference number
- Invoice date
- Fees
- Transaction number
- Payment type
- Payment status

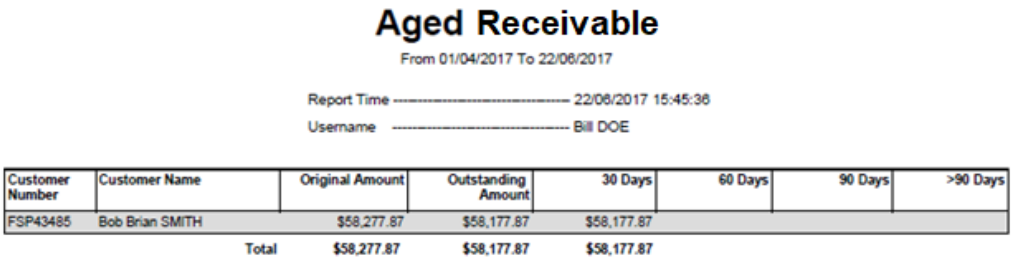
B. *Quick* Reports

Quick Reports uses Microsoft SQL Server Reporting Services to create system reports. Reports are generated automatically at the end of the day when output files are created for the accounting system. Reports can also be requested on an ad hoc basis.

Sample *Quick* Payments Reports

Aged Receivable Report

- This report is run to show debtors and the amount they owe and for how long an amount has been outstanding.
- Input parameter are date range.
- Fields included are Date report was run, Citizen Number, Citizen Name, Original Amount, Outstanding Amount, 30 Days, 60 Days, 90 Days, >90 Days, Original Amount Total, Outstanding Amount Total, 30 Days Total, 60 Days Total, 90 Days Total, and >90 Days Total.



Aged Receivable

From 01/04/2017 To 22/06/2017

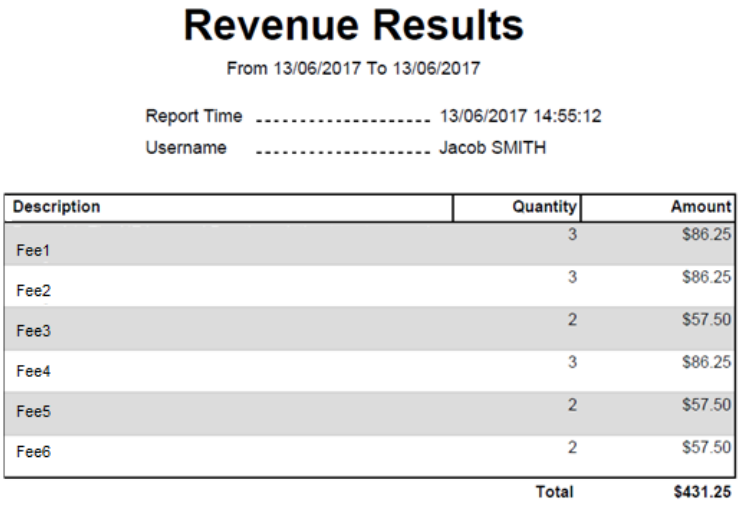
Report Time ---------- 22/06/2017 15:45:36
Username ---------- Bill DOE

Customer Number	Customer Name	Original Amount	Outstanding Amount	30 Days	60 Days	90 Days	>90 Days
FSP43485	Bob Brian SMITH	$58,277.87	$58,177.87	$58,177.87			
	Total	$58,277.87	$58,177.87	$58,177.87			

Figure 20 – Aged Receivable Report

Revenue Report

- This report shows revenue totals for all approved invoices paid or unpaid over a time period
- Input parameters are Date Range
- Fields included are Description, Quantity, and Amount.



Revenue Results

From 13/06/2017 To 13/06/2017

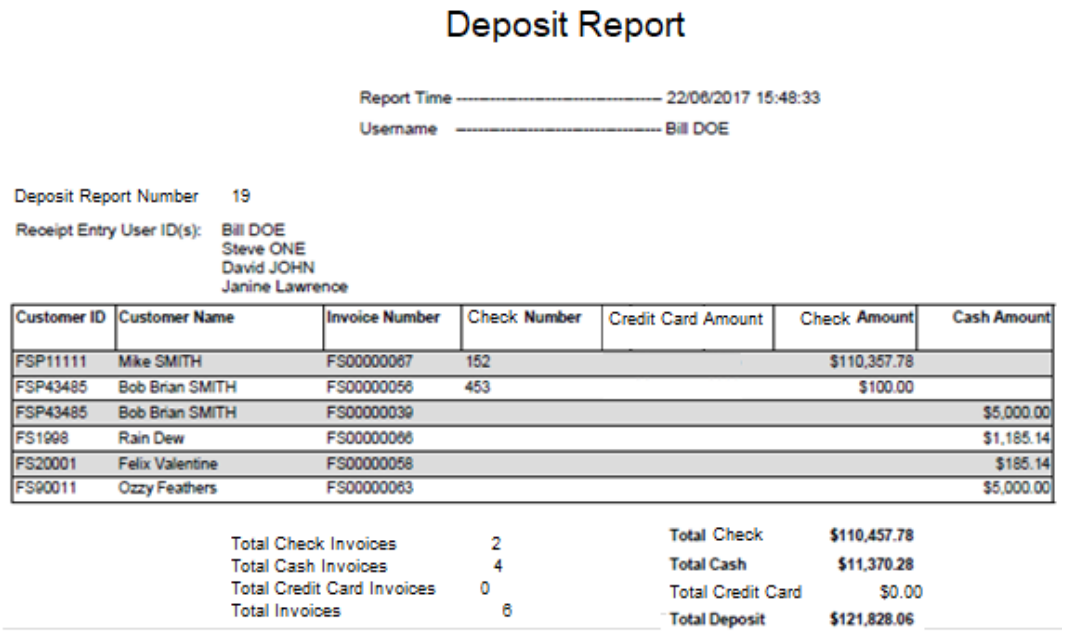
Report Time ---------- 13/06/2017 14:55:12
Username ---------- Jacob SMITH

Description	Quantity	Amount
Fee1	3	$86.25
Fee2	3	$86.25
Fee3	2	$57.50
Fee4	3	$86.25
Fee5	2	$57.50
Fee6	2	$57.50
	Total	**$431.25**

Figure 21 – Revenue Report

Bank Deposit Report

- This report is used as support documentation provided to the bank with the deposit slip for cash and foreign check deposits. Fields included are Receipt Entry User ID(s), Deposit Report Number, Citizen ID Citizen Name, Invoice Number, Check Number, Check Amount, Cash Amount, Credit Card Amount Total Deposit



Deposit Report

Report Time ---------- 22/06/2017 15:48:33
Username ---------- Bill DOE

Deposit Report Number 19

Receipt Entry User ID(s): Bill DOE
Steve ONE
David JOHN
Janine Lawrence

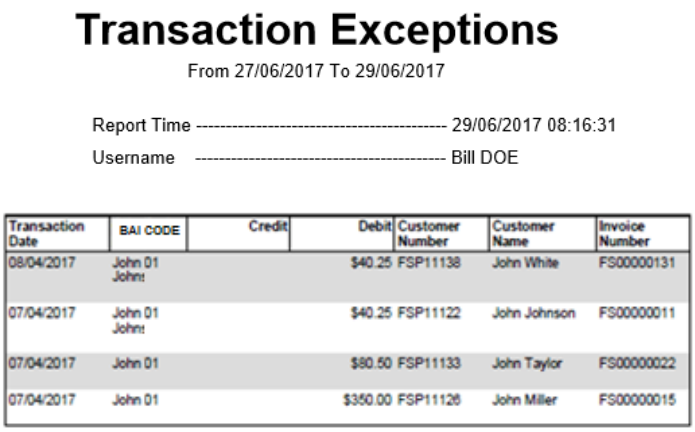
Customer ID	Customer Name	Invoice Number	Check Number	Credit Card Amount	Check Amount	Cash Amount
FSP11111	Mike SMITH	FS00000067	152		$110,357.78	
FSP43485	Bob Brian SMITH	FS00000056	453		$100.00	
FSP43485	Bob Brian SMITH	FS00000039				$5,000.00
FS1998	Rain Dew	FS00000066				$1,185.14
FS20001	Felix Valentine	FS00000058				$185.14
FS90011	Ozzy Feathers	FS00000063				$5,000.00

Total Check Invoices	2	**Total Check**	**$110,457.78**
Total Cash Invoices	4	**Total Cash**	**$11,370.28**
Total Credit Card Invoices	0	Total Credit Card	$0.00
Total Invoices	6	**Total Deposit**	**$121,828.06**

Figure 22 – Bank Deposit Report

Transactions Exceptions Matched Report

- This report provides the details for any payments received and any dishonors deducted on the bank statement that could not be matched to an invoice. It also shows when unknown payments have been identified and allocated to an invoice.
- Input parameters are Date Range
- Fields included are report Date, Transaction Date, BAI Code, Credit, Debit, Account Number, Citizen Name, Invoice Number



Transaction Exceptions

From 27/06/2017 To 29/06/2017

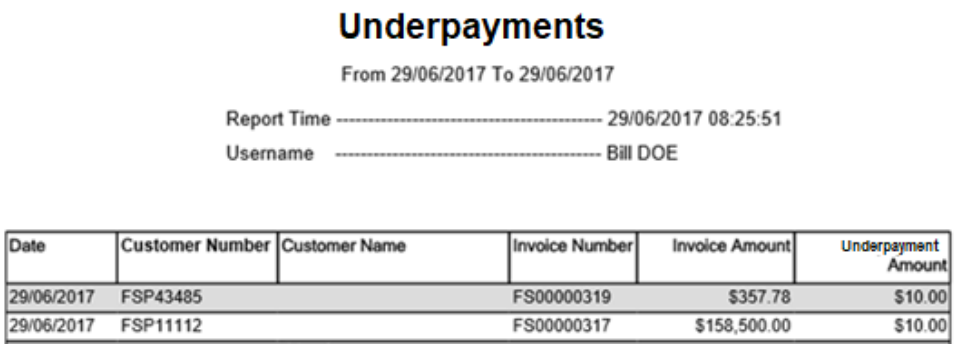
Report Time ---------- 29/06/2017 08:16:31
Username ---------- Bill DOE

Transaction Date	BAI CODE	Credit	Debit	Customer Number	Customer Name	Invoice Number
08/04/2017	John 01 John!		$40.25	FSP11138	John White	FS00000131
07/04/2017	John 01 John!		$40.25	FSP11122	John Johnson	FS00000011
07/04/2017	John 01		$80.50	FSP11133	John Taylor	FS00000022
07/04/2017	John 01		$350.00	FSP11126	John Miller	FS00000015

Figure 23 – Transaction Exceptions Matched Report

Underpayments/Overpayment Report

- This report is run to show any Underpayment/Overpayment above the invoice amount. Date range is according to Invoice Date.
- Input parameters are Date Range
- Fields included are Date report was run, Period report is for, Date, Account Number, Citizen Name, Invoice Number, Invoice Amount, Underpayment/Overpayment Amount



Underpayments

From 29/06/2017 To 29/06/2017

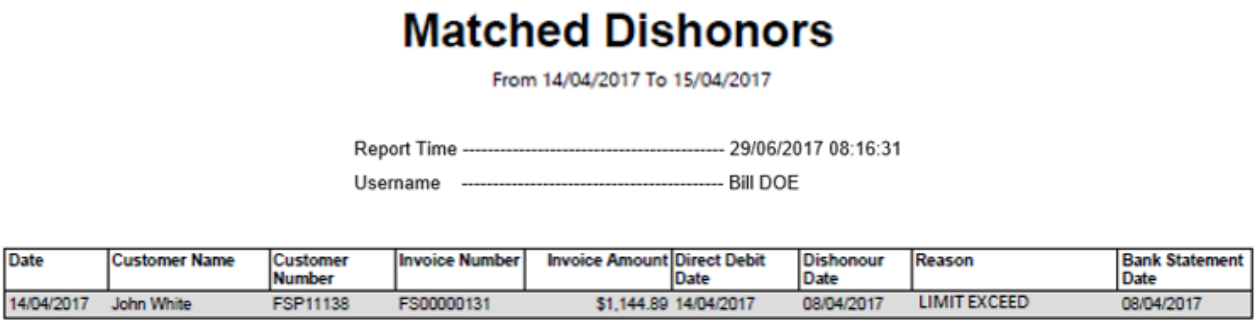
Report Time ---------- 29/06/2017 08:25:51
Username ---------- Bill DOE

Date	Customer Number	Customer Name	Invoice Number	Invoice Amount	Underpayment Amount
29/06/2017	FSP43485		FS00000319	$357.78	$10.00
29/06/2017	FSP11112		FS00000317	$158,500.00	$10.00

Figure 24 – Underpayments/Overpayment Report

Matched Dishonors Report

- This report is run to identify the Citizens whose ACH payments have failed and whose invoices have been reopened and passed to Finance
- Input parameters are Date Range
- Fields included are Date report was run, Date, Account Number, Citizen Name, Invoice Number, Invoice Amount, ACH Date, Dishonor Date, Reason, Bank Statement Date



Matched Dishonors

From 14/04/2017 To 15/04/2017

Report Time ---------- 29/06/2017 08:16:31
Username ---------- Bill DOE

Date	Customer Name	Customer Number	Invoice Number	Invoice Amount	Direct Debit Date	Dishonour Date	Reason	Bank Statement Date
14/04/2017	John White	FSP11138	FS00000131	$1,144.89	14/04/2017	08/04/2017	LIMIT EXCEED	08/04/2017

Figure 25 – Matched Dishonors Report

Credit Card Refund Report

- This report is run to provide the information needed to create a refund to a credit card
- Input parameters are Date Range and Merchant Number
- Fields included are Date report was run, Merchant Number, Period Report was Run for, Date, Citizen ID, Citizen Name, Invoice Number, Entity Number, Entity Name, Credit Note Number, Amount to be Refunded, Comment, Credit Note Authorizer

Credit Card Refund

From 21/06/2017 To 22/06/2017

Report Time ---------- 22/06/2017 16:14:58
Username ---------- David JOHN

Merchant Number: 90031909200

Date	Customer Number	Customer Name	Invoice Number	Credit Note Number	Amount to be Refunded	Comment	Credit Note Authorisor	Merchant Reference
22/06/2017	FSP11121	John Smith	FS00000079	000376	$1,206.22	tesr	Janine Lawrence	879 FS00000079 John Smith
21/06/2017	FS1998	Rain Dew	FS00000125	000348	$5,284.25	Credit Note on Paid Invoice	Janine Lawrence	90C FS00000125 Rain Dew
				Total	$6,490.47			

Figure 26 – Credit Card Refund Report

Refunds Raised Report

- This report is used by Finance to pay refunds to Citizens
- Input parameters are Date Range
- Fields included are report Date, Period report is for, Date, Account Number, Citizen Name, Bank Account Number, Refund Number, Comments, Fee Amount, Total Refund, Refund Requestor, Refund Authorizer

Refunds Raised

From 13/06/2017 To 13/06/2017

Report Time ---------- 13/06/2017 14:52:35
Username ---------- John Edelmann(MBIE Contractor - Fairfax)

Date	Customer Number	Customer Name	Bank Account Number	Refund Request Number	Comments	Total Refund	Refund Requestor	Refund Authorisor	Fee Amount
13/06/2017	FSP11112	Sarah JONES	asdf-0100011000000001	000333	test1	$6,071.36	John Edelmann (MBIE Contractor - Fairfax)	Bill DOE	$35.00
									$5,244.45
								Total	$5,279.45

Figure 27 – Refunds Raised Report

Audit Events Report

- This report is used for tracing all tasks made in *Quick* Payments
- Input parameters are Date Range, Audit Event Type, Username, Application
- Fields included are Date Time, Event Type, Username, Message, Application, IP Address, MAC Address

Audit Events

From 22/06/2017 00:00:00 To 22/06/2017 23:59:00

Report Time ---------- 22/06/2017 16:16:32

Username ---------- David JOHN

Date Time	Event Type	Username	Message	Application	IP Address	MAC Address
22/06/2017 16:15:59	ExecuteScheduledJob	Output Services	Executed job 'Reconcile Westpac File'.	QpayServices	10.0.12.1	0EC6F0B432CC
22/06/2017 16:11:12	Redirect	Bill DOE	Redirected from system 'FS' with operation Research.	WebApi	10.0.12.141	0EC6F0B432CC
22/06/2017 16:11:08	Logout	Bill DOE	User logged out.	Web	10.0.10.10	0EC6F0B432CC
22/06/2017 16:11:08	Return	Bill DOE	User exit Quick Payment System.	Web	10.0.10.10	0EC6F0B432CC

Figure 28 – Audit Events Report

C. *Quick* Payments Monitor

The *Quick* Payments Monitor provides real-time status of Payments received and the dollar value of each payment type. Real time status of files received by the system and automatic files generated by the system are included. Results are broken down by application.

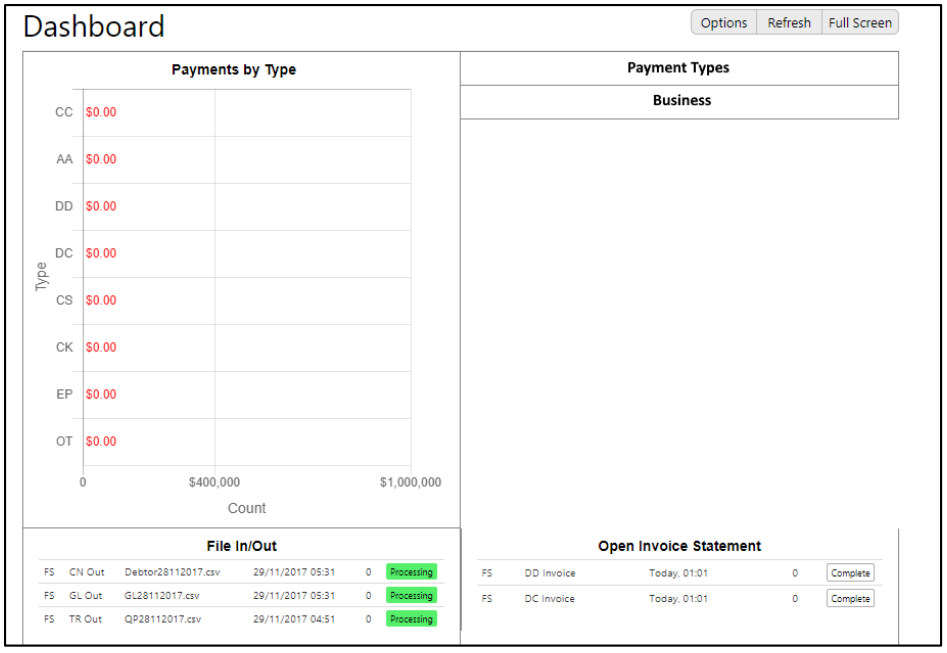


Figure 29 – *Quick* Payments Monitor Home Page

***Quick* Modules Cashier**

For in-person payments, the Fairfax Software solution includes *Quick* Modules Cashier. A web-based state of the art cashiering application that is an extension of *Quick* Payments. All payments processed by *Quick* Modules Cashier use the same integrations with the Parish's backend systems and all payments are consolidated into a single payments database.

***Quick* Modules Cashier Feature Set**

Quick Modules Cashier is one of the most feature-rich products of its kind in the market. The most prominent distinguishing characteristics that set *Quick* Modules Cashier apart from the competition are distributed along several attributes. These are:

✓ **Architectural Attributes:**

1. All transactions companywide are managed by a centralized Microsoft SQL database.
2. Service-Oriented Architecture allows integration with external systems via web services APIs.
3. Web-based for easy deployment and support and providing the Parish with web-based cashiering, configuration management, daily reporting. No application software is installed on the workstation.
4. The FFX Client Communicator API is executed on the workstation to connect cashiering hardware to the web-based cashiering application. This allows each workstation to have a unique hardware configuration.
5. Deployment in multiple environments – Development, Test, and Production.
6. Three-tier architecture offering many benefits:
   - **Security:** Can be isolated to limit access and exposure.
   - **Availability:** Each tier is independent from the other tiers; this provides the benefit of not having a single point of failure.
   - **Scalability:** Each tier can be scaled as desired without affecting the other tiers.
   - **Flexibility:** Each tier can be managed or scaled independently giving the system increased flexibility.

✓ **Security Attributes:**

6. Secure PCI and SOC2 compliant environment
7. Supports and utilizes secure communications for internet-based transactions using HTTPS over secured network connections.
8. Adheres to Government Accounting Standards Board (GASS) principles as described in http://www.gasb.org/home.
9. Data encryption at rest and in transit following Federal Information Processing Standard (FIPS) Publication 140-2 standards (FIPS PUB 140-2).

✓ **Ergonomic Attributes:**

1. Supports touch screen and/or keyboard entries.
2. Creates a real-time electronic receipt displayed on the screen, sent via email and/or SMS Text and/or printed at the cashiering workstation.
3. Creates payment receipts – each receipt has configurable elements so each cashiering location may have a unique receipt definition.

4. Accepts all US legal tender including cash, checks, money orders, debit, and credit cards.
5. Automatically identifies foreign checks that can be accepted or rejected per Parish business rules.
6. Convenience fees (if any) for debit/credit card transactions are added to the receipt as a separate line item.
7. Compatible with a wide variety of smart terminals that support the latest card EMV chip technology and Near Field Communications to contactless payments as well as popular digital wallet payment methods such as Apple® Pay and Google® Pay.

✓ **Workflow Attributes:**

7. Provides remote real-time monitoring of workstation status controlled by login privilege.
8. Provides automatic general ledger entries in a file-based transfer to the Parish's accounting systems.
9. Provides automated output of payment files on a schedule set by the Parish. Files are verified before they are sent automatically. Functions are provided to handle exception conditions.
10. When a cashiering batch is closed, checks are automatically queued for ACH deposit to the preferred bank. Checks captured in all locations are consolidated into a centralized ACH process for electronic deposit to one or more banks.

✓ **Cash Management Attributes:**

1. Accepting cash is a configurable option by workstation.
2. Compatible with automatic cash drawers.
3. All cash in and cash out amounts are automatically tracked and audited.
4. Manages cash inventory with audit reporting for all cash movement including:
   a. From the bank to the cash vault
   b. From the cash vault to Beginning of Day cash for each cashier
   c. Intra-day transfer from the vault to a cash drawer balance falls below the desired level
      i. A manager is notified when the cash drawer balance falls below the desired level
   d. Intra-day transfer from the cash drawer to the vault when cash-on-hand rises above the desired level.
      i. A manager is notified when the cash drawer balance rises above the desired level.
   e. End of day transfer of cash from the cashier to the cash vault
   f. From the vault to the bank
5. A cashier may perform a system assisted trial balance at any time.
6. Cash drawers are assigned to a cashier logically and can be moved from workstation to workstation as needed.

✓ **Cashier Batch Attributes:**

1. Provides comprehensive and separate research features for cashiers and managers for open and closed batches.

2. Cashiering batches are tied to a Cashier user-id allowing cashiers to move from workstation to workstation without closing the batch.
3. A manager may take control of a batch from the current user to balance and close the batch.
4. A manager can track the balance of all cash drawers in real time.
5. A manager can track cashier productivity in real time.
6. During End-of-Day procedures, out-of-balance batches can only be adjusted with manager approval.

✓ **Cashier Transaction Attributes:**

1. A transaction is not complete until it is in balance, as defined by Parish specific business rules.
2. A cashier can suspend the current transaction at any time and start a new transaction.
3. A suspended transaction can be reopened and completed any time before batch closeout.
4. A suspended transaction can be reopened and completed by a manager or another cashier.
5. A completed transaction can be reopened any time before batch closeout.
6. A transaction is made up of one or more coupons and fees and one or more payment methods that balance.

✓ **Connectivity Attributes:**

1. Connects to host systems via Web Services APIs or Open Database Connectivity (ODBC) to provide automatic lookup and verification of billing data.
2. Provides interfaces to backend systems to post payments, void payments, and lookup bill information.
3. Integrates with the Parish legacy imaging system (if any).
4. All card transactions are authorized in real-time regardless of the transaction amount.

✓ **Audit Tracking Attributes:**

1. Tracking transactions from receipt all the way through the entire processing pipeline to output.
2. Multilevel approval workflow is available for required processes. For example, approval can be required before a cashier can initiate a void.
3. Robust comprehensive reporting based on Microsoft SQL Server Reporting Services (SSRS).
4. Full logging (verbose and summary) capability.
5. Full audit tracking reporting.
6. Standard and customized reports by cashier and reports consolidated by location and companywide.
7. Maintains the integrity of the database and transactions in case of power failure or abrupt shutdown.
8. Provides the ability to restart and recover after an abrupt shutdown or power failure without loss of data or software components.

9. Provides a full audit trail of all transactions, record changes, and user logins.
10. Provides the ability to re-print receipts. All re-printed receipts are identified as a duplicate/re-print of the original.
11. Provides a method to reverse transactions including those systems it is integrated with.
12. Provides a method, controlled through security, of correcting or adjusting a transaction previously posted. Allows the operator to alter/update fields, issue a void of the original transaction and post the new transaction to keep the audit trail intact.
13. Allow all reports to be exported in common formats including but not limited to, Microsoft Excel, Microsoft Word, Adobe PDF, Comma Separated Values (CSV), Extensible Markup Language (XML), fixed field text (TXT), JavaScript Object Notation (JSON).
14. Provides payment statistics. For example, number of payments processed in a given time, number of payments processed by a station in a given time, number of bills of type X processed in a given time, average time to process a payment, etc.

✓ **Versatility Attributes:**

1. Ability to process credit/debit card payments is optional by workstation.
2. Ability to accept payments by cash and cash drawer management is optional by workstation.
3. Ability to configure specific check/OCR readers by workstation.
4. Ability to configure receipt printers by workstation.
5. Future proofed allowing the Parish to use virtually any cashiering hardware device including cash drawers, receipt printers, check/OCR scanners, barcode readers, and credit card smart terminals.
6. Card processor agnostic, allowing the Parish to work with the merchant service provider of the Parish's choice.
7. Provides substitute document images if a scanned image is not available.
8. Provides the ability to handle multiple fund accounting.
9. Does not place limits or restrictions on the number of items to pay in one transaction.
10. Does not place limits or restrictions on the number of payment methods used in one transaction.
11. Compatible with a wide variety of smart terminals that support the latest card EMV chip technology and Near Field Communications to contactless payments as well as popular digital wallet payment methods such as Apple® Pay and Google® Pay.

Cashiering Workstations

Quick Modules Cashier workstations that receive in-person payments are staffed by Parish employees at various department locations including

- Jefferson Protection and Animal Welfare Services (JPAWS)
- Alario Center
- Code Enforcement
- Planning Department
- Recreation Department
- Library

The workstation configuration provides full cashiering functionality:

- Modern design that supports touch screen monitors
- A keyboard and mouse are supported but not required
- Web-based for easy deployment and support
- Cash drawer support with balancing tools
- Compatible with virtually all Cashiering peripherals
- Supports check and document scanning but not required
- Accepts all legal tenders including cash, checks, debit cards, credit cards
- Accepts mobile based digital wallet payments including Apple Pay, Google Pay, and PayPal
- Card transactions via swipe and EMV chip technology
- Full featured easy to customize receipt with all transaction details
- User defined transaction keys
- Account lookup with real time integrations with Parish backend systems

Cashiering Hardware

Quick Modules Cashier is compatible with virtually all existing cashiering hardware owned by the Parish. The recommended cashiering hardware includes:

Cashiering Hardware	Description
 ELO 1715LTouchscreen Monitor	*Quick* Modules Cashier is compatible with any MS Windows compatible monitor. Fairfax Software recommends a 17" display
 Epson TM-U220 Receipt Printer	The Epson TM-U220 is a dot matrix impact printer that uses standard paper that features print that will not fade over time.
 APG Series 4000: 18126 Cash Drawer	For locations that take cash payments, *Quick* Modules Cashier features full management of the cash drawer.
 MagTek Excella STX	For locations that accept checks, the Excella STX is a small footprint single feed scanner that captures the front and back of checks for electronic deposit and coupons.

Credit Card, Debit Card, and Digital Wallet Processing

The Fairfax Software solution includes Visa, MasterCard, Discover, and American Express card processing through Govolution. Govolution will provide all merchant services for the project using Point to Point Encrypted Devices (P2PE) for card present and digital wallet transactions.

Why P2PE?

P2PE is an added layer of protection for point-of-sale transactions. Payment data and cardholder information is immediately encrypted upon tap, dip, swipe or key entry in a P2PE-certified device. Encryption is done outside of *Quick* Modules Cashier and stored offsite in a Hardware Security Module (HSM), preventing clear-text cardholder data from being visible and providing an extra layer of security for your customers.

We offer two Point to Point Encryption (P2PE) solutions. Either P2PE or P2PE Verified. The difference between the two is that P2PE Verified means verification through an approved 3rd party P2PE accessor to ensure security. If only P2PE is required, there would be no cost for the terminals, IPP320, or any other additional costs associated. Either P2PE solution is the gold standard of payment security, delivering the most reliable payment security in the industry. Validation of compliance is available upon request.

P2PE Devices:

The list of P2PE devices are provided at no cost.

Device	Description
 Ingenico IPP320	The Ingenico IPP320 includes, Key, Swipe, EMV and Contactless payments. It features a 1 in x ¾ in screen with no signature capture.
 SwipeSimple B250 for Smartphones and Tablets	The SwipeSimple B250 supports ✓ EMV and magnetic stripe card types ✓ Contactless tap-to-pay cards and mobile payments ✓ Bluetooth Low Energy securely connects to iOS or Android mobile devices

P2PE Verified Devices:

P2PE Verified devices provide verification from an approved 3rd party verifier. The cost of these devices is included in the cost section.

Device	Description
 Ingenico Lane 3000	The Ingenico Lane 3000 includes, Key, Swipe, EMV and Contactless payments. with a 2.8” screen with no signature capture.
 Ingenico Lane 5000	The Ingenico Lane 5000 includes, Key, Swipe, EMV and Contactless payments. with a 7” screen with signature capture.

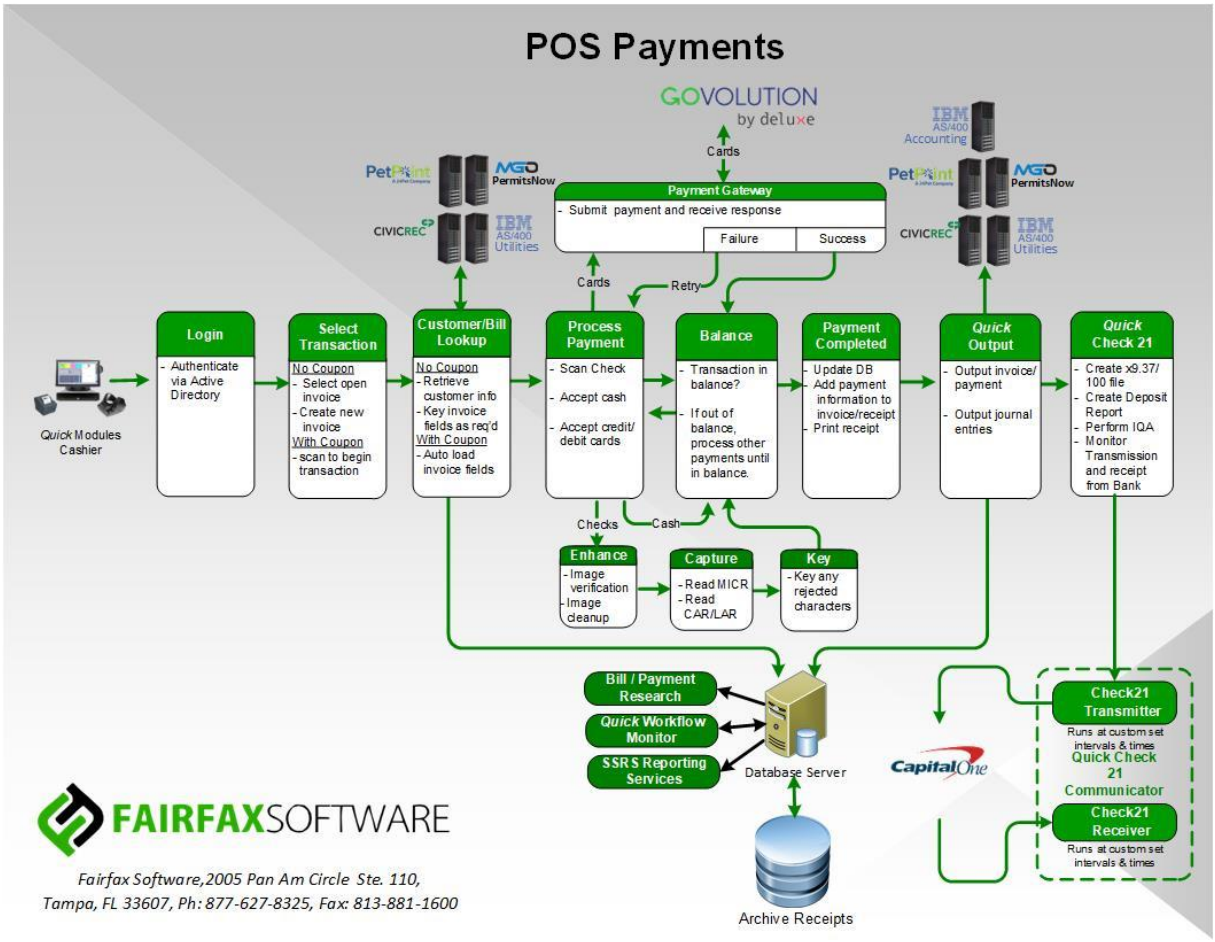


Figure 30 – Cashiering Workflow

Transaction Workflow:

1. Login - Cashier login via Active Directory. The user is authenticated following the rules for the login method.
2. Determine Transaction Type
    - Fixed Fee Transaction – Transaction buttons will represent fixed fee transactions like parking passes, one-time permits, or miscellaneous charges. The operator selects the desired transaction button, and the fee is automatically recorded.
    - With a Utility Bill – the cashier selects the transaction type r scans the coupon to initiate the transaction.
    - With a customer lookup – The *Quick* Modules Cashier operator will select a button to determine the transaction type and perform a customer lookup via API connection to the Parish system that supports the location. Once a fee is selected to pay, payment details will automatically download and populate into fields on the screen. The cashier will key any other required data for processing.

- More than one transaction entry can be added to the shopping cart. For example, two fees are paid by a single check.

3. Tender Payment - The customer tenders payment with an option that is valid for the transaction type. More than one payment option can be selected that adds up to the total due.
    - Checks – the cashier enters the check number, bank number, account number, and the amount into the cashiering screen. If the optional check scanner is used, press the scan button and drop the check into the scanner.
    - Debit Cards, Credit Cards, and digital wallet transactions will be processed on the credit card terminal provided by Govolution. This will include Debit Cards, Credit Cards, and digital wallet transactions such as Apple Pay and Google pay.
    - Cash – Cash-In and Cash-Out amounts are recorded by the system. Cash Drawer management from the cash vault to deposit is provided.
4. Balance the Transaction - The transaction is balanced automatically. If the transaction is not balanced, additional payments can be processed until the transaction is in balance. Balanced transactions are then updated in the database.
5. The transaction receipt is printed and/or emailed to the customer.

Cashiering Screens

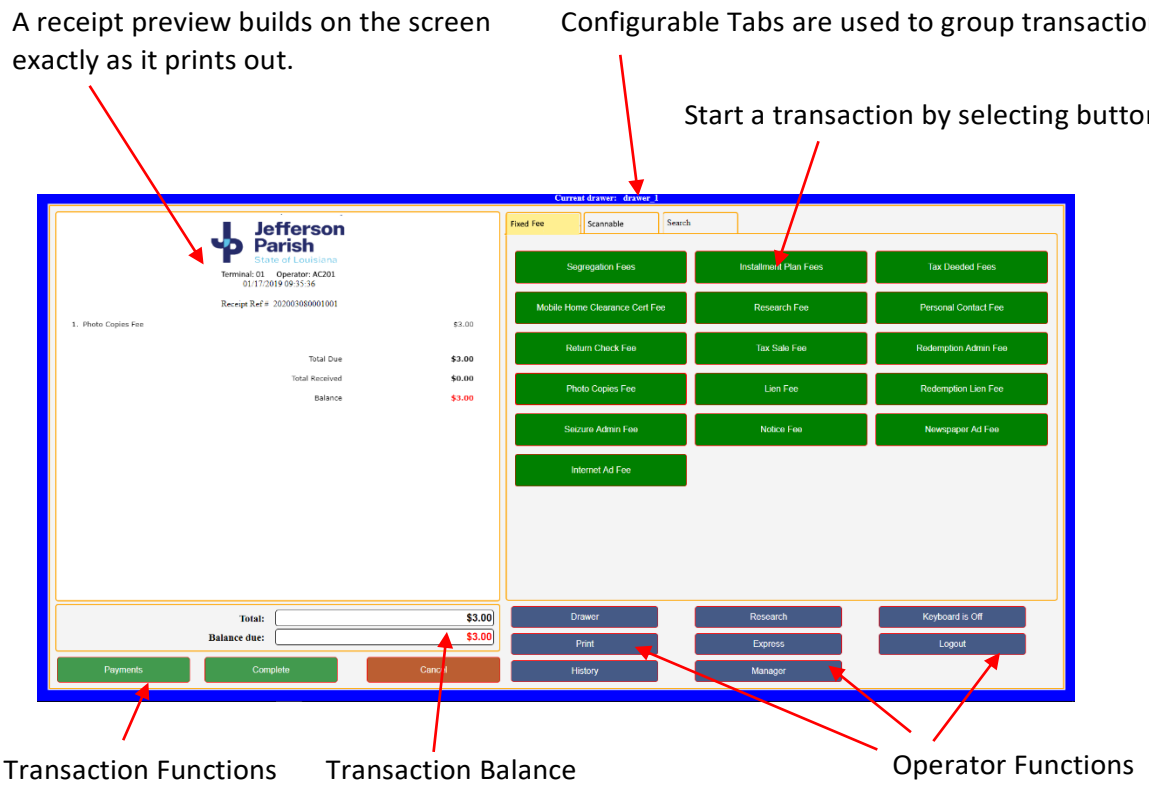


Figure 31 – Main Cashiering Screen

Designed for ease-of-use, the *Quick* Modules Cashier cashiering screen is compatible with touch-screen hardware. Entries can be completed from the screen or a keyboard.

The main screen features configurable tabs for grouping transaction types together. There is no limit on the number of buttons or tabs. Using the Search Tab, a cashier can quickly navigate to a desired tab.

Point-and-Click Setup

The cashiering screen is configurable so that each cashiering workstation is customized for its location to exact Parish requirements. Access is controlled by operator login. For example, the Utility Tab contains utility payment types and can be visible only to Utility Cashiers and Library Transactions are defined on the Library Tab, only accessible to Library cashiers. All tabs can be visible to supervisors or accounting personnel.

Payment types are represented by screen buttons. Buttons can be setup to pre-load data for permits, taxes, decals, or other collections that are a fixed cost. Other buttons are set up to require entry of specific fields and variable amounts. Customer account lookups can be defined to pull billing data from host systems for payment. There is no limit to the number of buttons and tabs that can be set up within *Quick* Modules Cashier.

Configurable Receipt

Fields on the receipt are customizable by workstation and location. In addition to the logo, user configurable free form messages can be printed on the receipt at the beginning and the end of a transaction.

The Parish has control of lines that print for individual transaction types that can include document fields such as Account Numbers, Document Locator Number, or any other database field associated with the transaction.

A receipt can be printed on the receipt printer and/or emailed to the payer. A duplicate receipt can be printed and includes the words “Duplicate Receipt” to indicate the receipt is a duplicate.

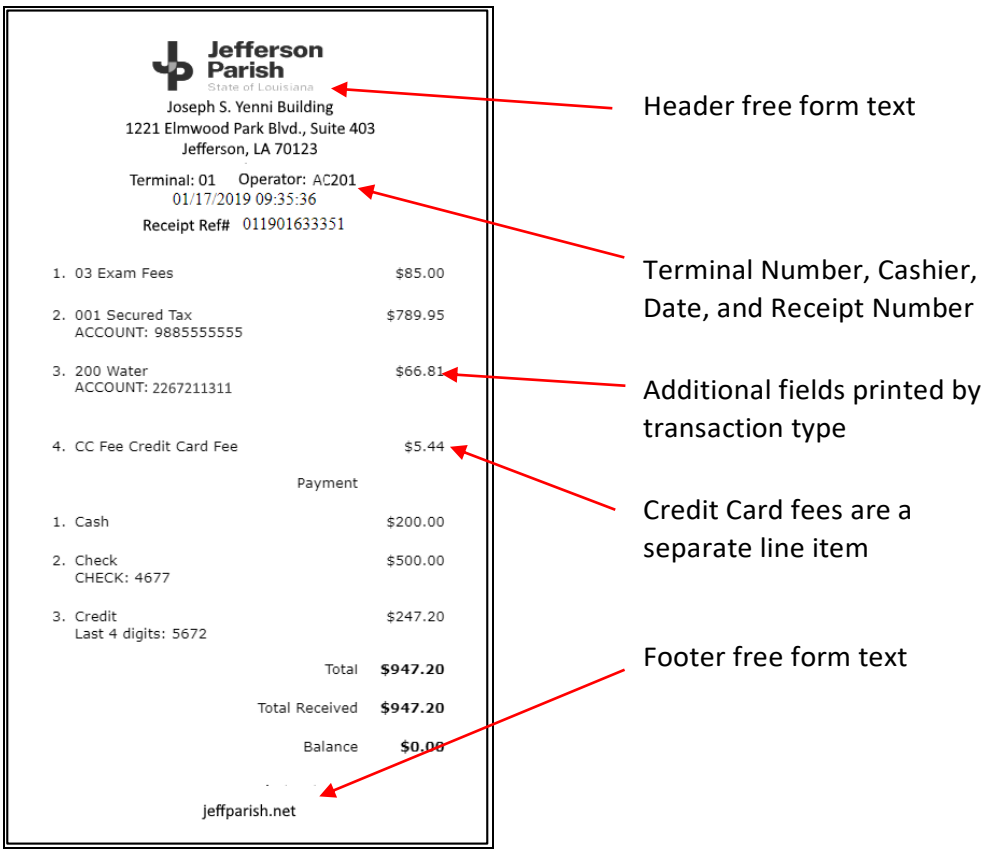


Figure 32 – Customizable Receipt Layout

Cash Vault Management

Quick Modules Cashier includes cash vault management for locations that accept cash. Each cashiering location is assigned a cash vault, typically a workstation that manages cash on hand for the location. Cash deposited in the cash vault and cash distributed from the cash vault to other cashiers is balanced and recorded in the system audit. All events are tracked, including cash received from the bank, beginning of day cash distributed to cashiers, additional cash-out or cash-in as needed by cashiers during their shift, end of day cash deposited from each cashier, and cash transferred from the vault for deposit to the bank.

Cash Drawer Management

Quick Modules Cashier includes cash drawer management. Cash is tracked starting with setting up the cash drawer when a cashier begins a shift, adding and subtracting cash throughout the day, and finally balancing the cash at the End of the Day (EOD). A supervisor login is required to approve the beginning cash counts. Each cashier is required to end the day in balance with a supervisor override option available.

A cashier can perform a Trial Balance anytime during the day, as required. Supervisors can track the cash balance in each cashier's drawer from a different location. End of day procedures require each cash drawer to balance at the end of each shift.

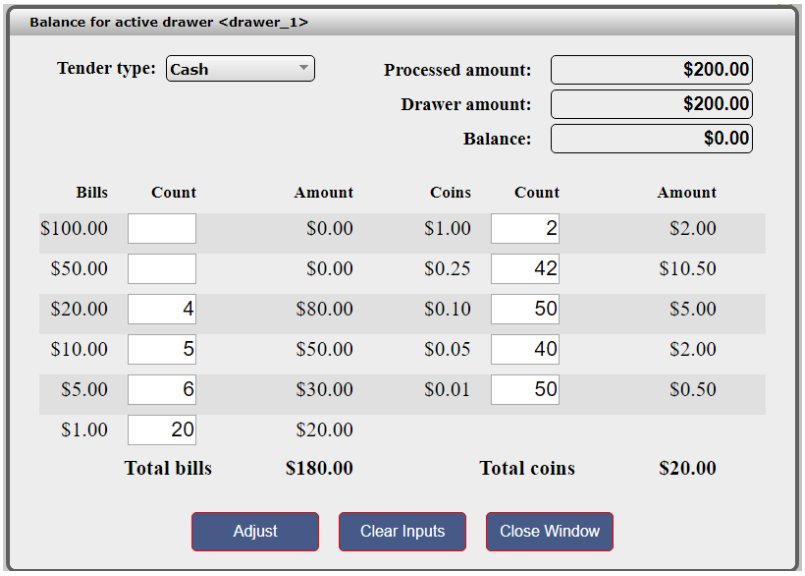


Figure 33 – Cash Drawer Balancing

Cash drawers can be moved from one workstation to another during the day. A workstation can be configured with multiple cash drawers. Cash drawers can easily be swapped when a cashier goes on break. When a cash drawer is active, a unique color assigned to the cash drawer displays as a screen border along with the active cash drawer name to quickly indicate which cash drawer is currently active.

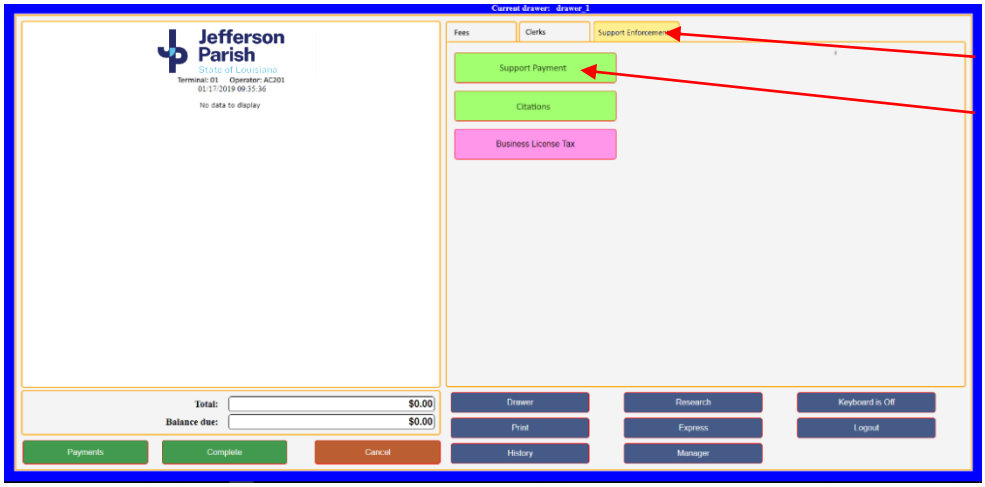
Figure 34 – Swap Cash Drawers

Transaction Options

There are two basic types of transactions – payment of a bill and fixed fee transactions that purchase a service or item, such as a parking sticker or permit.

- Payment of an Amount Due/Liability

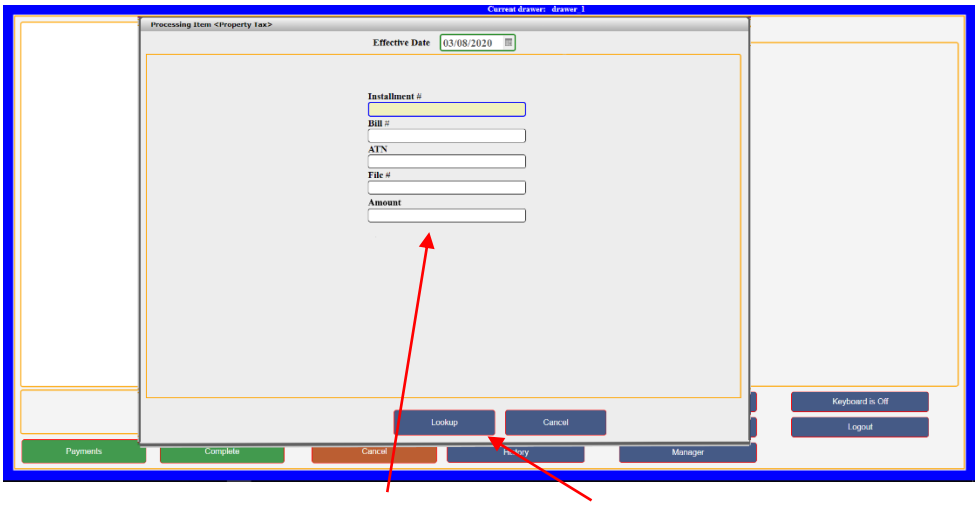
Transactions are started by selecting a transaction type button on the screen that is assigned to the type of transaction to be processed.



1. Select Tab
2. Select transaction button

Figure 35 – Select Transaction Button

If the cashier has documentation or an invoice that documents the amount due, the cashier will select the transaction type and enter the transaction details on the screen. Each transaction type can be configured to process the many different payment types processed by the Parish.



Enter Fields or Lookup Customer Record

Figure 36 – Scan or Lookup

As fields are entered, they are validated based on the business rules established within *Quick* Modules Cashier and populated into the fields on the screen. The cashier will correct any fields that fail validation.

Once the form is accepted, then payment is rendered and balanced to the total amount due. Business rules are set to control how partial payments and overpayments are to be processed. The procedures can be unique for each remittance type and client.

- Customer Lookup

  For transactions where a lookup is required, the system can be configured to look up customer information on one or more host systems. Since *Quick* Modules Cashier is web-based, connections to third party systems can be easily achieved using an API or other industry standard connection methods. Once a lookup has identified the customer, information is automatically copied into the transaction screen.

  The cashier will use the name and address information to verify customer identity. Liabilities in the system are automatically listed. Once the operator hits the OK button indicating that the customer information is correct, the liabilities are automatically entered into the system for payment. The cashier can then process the payment.

- Fixed Fee Button

  The cashier can select a transaction button to start a new transaction. The Payment Type and fixed fee amount loaded for the transaction is automatically entered into

the transaction. The cashier can perform a customer lookup to add the customer's information to the transaction if it is required. Transaction workflows will be set to match the Parish's business rules. Once the transaction is entered, then payment is rendered.

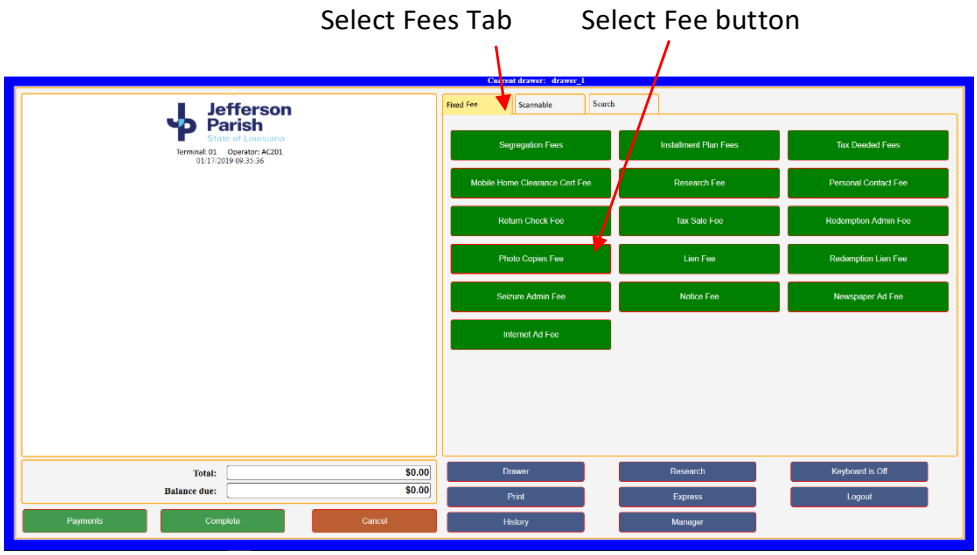


Figure 37 – Select Fee Button

After the Fixed Fee Button is selected, the amount is automatically added to the transaction and recorded to the receipt.

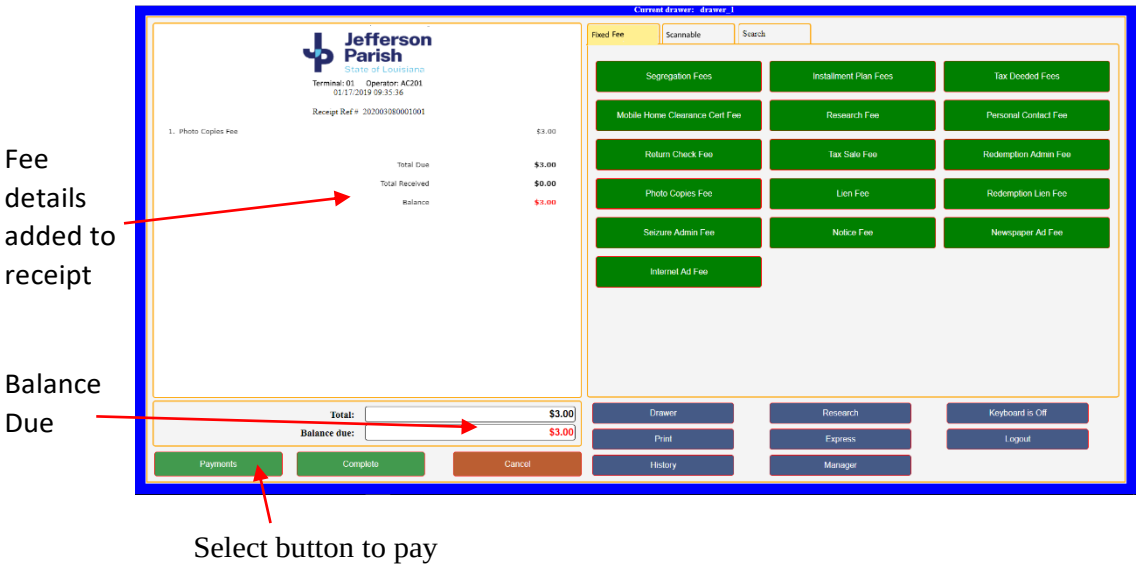
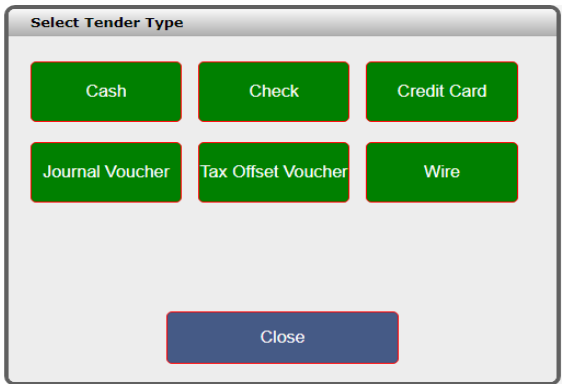


Figure 38 – Accept Fee

Payment Options

Quick Modules Cashier accepts all forms of payments including cash, checks, money orders, credit cards and debit cards, and ApplePay® and Google Pay®. A single payment can be applied across multiple transaction types. If multiple tender types are presented for a payment, the system will automatically tally the payments and balance the amount to the transaction. A full audit trail is provided for each transaction and recorded on the receipt.



Tender Types available for a payment are filtered by Transaction Type. Only those options that are valid for this transaction Type are shown.

Figure 39 – Select Tender Type

- Cash

  For cash received, the cashier enters the bills and coins received by denomination to verify the amount received before adding the cash to the cash drawer. This is a feature that can is activated by cashier.

  For change due, the system will automatically display the change due and provide a bill and coin count for the cashier to retrieve from their cash drawer. This is a feature that is activated by the cashier.

- Checks and Money Orders

  Checks and money orders are scanned and the MICR data and the check amount are read. The check is endorsed electronically. Data is automatically populated into the transaction screen for cashier review. Check data is verified against the *Quick* Modules Cashier SQL database to ensure that it is not a duplicate. Internal and external databases can also be checked to verify bank and account information and to make sure the account is not on the NSF hot list or is a known fraudulent account. If the check is a duplicate or found on a hot list, the cashier is automatically notified, and the check is not accepted. The transaction can be completed with another form of acceptable payment.

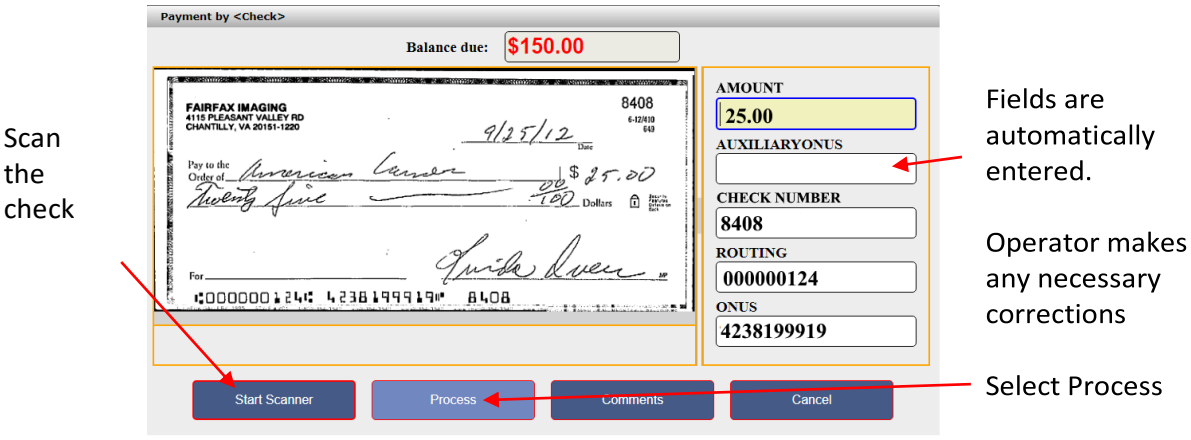


Figure 40 – Scan a Check

- Foreign Checks

  Foreign checks are automatically identified and processed according to Parish business rules. The system can be setup to accept or reject the check. If checks are accepted, they are prepared for manual deposit.

- Debit and Credit Cards

  Following payment card industry standards and security requirements, all major cards can be used for payment including Visa, MasterCard, Discover, and American Express branded debit and credit cards can be used for processing card transactions. Using the selected P2PE terminal, the credit card is swiped, or the chip scanned by the smart card reader to capture, and process required fields. The cashier also has the ability to manually enter the fields if the read is invalid. Card numbers are validated using the check digit routines used by the respective credit card providers. A connection to the Govolution card terminal provides card and digital wallet validation and processing of the amount. Approval codes and transaction information are stored in the *Quick* Modules Cashier Database for reporting and processing downstream.

  The Payment Workflow processes payments directly to Govolution. No PCI data is stored in the *Quick* Modules Cashier database. Tokens are saved in lieu of personal data should a payment need to be voided.

  Credit card charges and convenience fees are assigned by payment type. Credit card fees are charged to the customer and added to the receipt as a separate line item. The fee amount is displayed to the customer prior to processing the transaction. The customer can choose to cancel the transaction and pay another way if they do not accept the fee amount. The following example shows how a typical point-to-point encryption device is used by *Quick* Modules Cashier.

- Digital Wallet Payments

  Mobile wallet payment methods are supported using the contactless payments capability of the credit card terminal. Support includes Apple Pay™ and Google Pay. Other digital payment methods can be added as they become available.

All transactions are time stamped and assigned a unique receipt number and a Document Locator number for each line item paid. Recorded with each transaction is the Location, Workstation ID, the Cashier ID, and along with all transaction data. The receipt layout is configurable by workstation. The receipt can be customized to the Parish's specifications.

Cancelations and Voids

- Same day

  A line item or the entire transaction can be canceled before a transaction is completed. If cancelled, the transaction is not added to the batch.

  If the transaction has been completed and added to the batch, it can be retrieved and voided before end of day processing is complete. If voided, the transaction will not be output to the host, any card transactions are removed from the settlement file, and, if the Check 21 optional feature is included, any checks are removed from the Check 21 deposit.

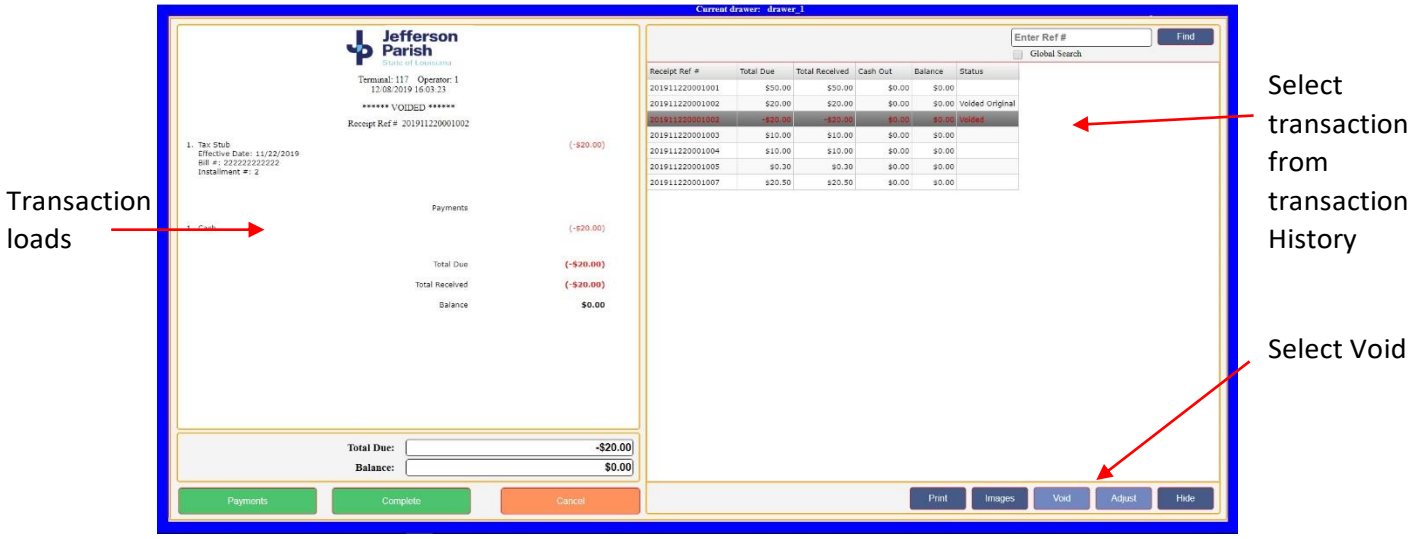


Figure 41 – Void Transaction

- Next Day

  A transaction can be retrieved and voided the next day. A reversing transaction is processed to reverse the line items and payments in the original transaction following the Parish specific business rules.

Other Features

- Manual override of the Settlement Date
- Transactions can be suspended and reopened for later completion

Reports

Standard cashiering reports are generated automatically or on demand. Reports are created using Microsoft SQL Server Reporting Servicers (SSRS). Standard Reports will be customized to match the Parish requirements.

Sample Standard Cashiering Reports

Cashier Fee Deposit Summary Report. This is a summary report for all cashiering batches for each tender type collected.

QUICK Reports

Cashier Drawer Balance Tender Summary Report

From 8/18/2020 to 8/18/2020

Location ID	Drawer ID	Count	Payment Type	Amount
LocMainOffice	Drawer 01	3	Cash	$79.00
		0	Check	$0.00
		2	CreditCard	$30.75
		0	Journal Voucher	$0.00
		0	Tax Offset Voucher Check	$0.00
		0	Wire	$0.00
	Drawer 01 Total	***5***		***$109.75***
	Drawer 02	1	Cash	$15.00
		1	Check	$2,861.05
		2	CreditCard	$2,307.44
		0	Journal Voucher	$0.00
		0	Tax Offset Voucher Check	$0.00
		0	Wire	$0.00
	Drawer 02 Total	***4***		***$5,183.49***
Grand Total:		**9**		**$5,293.24**

Cashier Payment Summary Report. This is a summary report for all payment collected by cashiering location.

QUICK Reports

Cashier Payment Summary Report

From 8/18/2020 to 8/18/2020

Location ID		Count	Payment Type	Amount
LocMainOffice		4	Cash	$94.00
		1	Check	$2,861.05
		4	CreditCard	$2,338.19
		0	Journal Voucher	$0.00
		0	Tax Offset Voucher Check	$0.00
		0	Wire	$0.00
	SubTotal:	**9**		**$5,293.24**
Grand Total:		**9**		**$5,293.24**

Cashier Supervisor Cash Drawer Report. This is a report by operator and cash drawer of all cash, cards, checks, and other tender types received.

QUICK Reports

Cashier Supervisor Cash Drawer Report

From 8/18/2020 to 8/18/2020

Operator ID	Workstation	Cash Drawer ID	Num Checks Trans	Num Debit/Credit Trans	Num Cash Trans	Cash Drawer	Other	Total
cashier3	123	Drawer 02	1	2	1	$15.00	$5,168.49	$5,183.49
cashier2	123	Drawer 01	0	2	3	$87.00	$30.75	$117.75
			1	4	4	$102.00	$5,199.24	$5,301.24

Cashier Fee Deposit Summary Report. This report provides a summary of fee types collected by batch.

QUICK Reports

Cashier Fee Deposit Summary Report

From 8/18/2020 to 8/18/2020

Batch Number	Operator	Count	Type	Total
CAS202008180001	Cashier2	2	ValleyRide Pass	$84.00
		1	Parking Ticket	$15.00
		1	Research Fee	$10.00
		2	Service Fee	$0.75
		Total for CAS202008180001		
		6		**$109.75**
CAS202008180002	Cashier3	2	Parking Ticket	$30.00
		1	Sample Property Tax	$5,097.21
		2	Service Fee	$56.28
		Total for CAS202008180002		
		5		**$5,183.49**
Grand Total:		**11**		**$5,293.24**

Cashier Payment Summary Report. This is an End of Day report that breaks down total fees and payments by type.

QUICK Reports

Cashier Supervisor End of Day Report

From 8/18/2020 to 8/18/2020

Type Count	Type	Description	Type Total
4	023	Service Fee	$57.03
1	027	Research Fee	$10.00
1	042	Sample Property Tax	$5,097.21
3	044	Parking Ticket	$45.00
2	048	ValleyRide Pass	$84.00
11		Type Grand Total:	$5,293.24

Payments Count	Payments Type	Payments Total
4	CASH	$102.00
1	CHECK	$2,861.05
4	CreditCard	$2,338.19
9	Payments Grand Total:	$5,301.24

Beginning Vault Balance	$543.00
Cash-In	$8.00
Cash-Out	-$543.00

Cash Drawer Report. This report describes the cash drawer balance by cashier.

QUICK Reports

Cash Drawer Report

From 8/18/2020 to 8/18/2020

Beginning Cash

Operator	Bill	Count	Amount	Coins	Count	Amount
Jsmith						
	$100	1	$100.00	.25	80	$20.00
	$50	2	$100.00	.10	50	$5.00
	$20	5	$100.00	.05	80	$4.00
	$10	10	$100.00	.01	100	$1.00
	$5	10	$50.00			
	$1	20	$20.00			
		Total Bills	$470.00		Total Coins	$30.00

Cash Position		
	Beginning Cash	$500.00
	Cash In	$3,020.00
	Cash Out	($10.00)
	Ending Cash	$3,010.00

Cashier Transaction History Report. This report provides detail on all transactions processed within a cashiering batch.

QUICK Reports

Cashier Transaction History Report

From 8/18/2020 to 8/18/2020

Batch Number: CAS202008180002

Operator: cashier3

Receipt Number: 202008180002002 **Time: 8/18/2020 11:23 AM**

Type	Amount	PayType	Amount	
Starting Cash	$243.00			
		Cash	$243.00	
Total Type:	$243.00	Total Paid:	$243.00	**Status: Paid**

Receipt Number: 202008180002003 **Time: 8/18/2020 11:25 AM**

Type	Amount	PayType	Amount	
Parking Ticket	$15.00			
		Cash	$15.00	
Total Type:	$15.00	Total Paid:	$15.00	**Status: Paid**

Receipt Number: 202008180002004 **Time: 8/18/2020 11:27 AM**

Type	Amount	PayType	Amount	
Parking Ticket	$15.00			
Service Fee	$0.38			
		Creditcard	$15.38	
Total Type:	$15.38	Total Paid:	$15.38	**Status: Paid**

Receipt Number: 202008180002005 **Time: 8/18/2020 12:31 AM**

Type	Amount	PayType	Amount	
Sample Property Tax	$5,097.21			
Service Fee	$55.90			
		Check	$2,861.05	
		Creditcard	$2,292.06	
Total Type:	$5,153.11	Total Paid:	$5,153.11	**Status: Paid**

Receipt Number: 202008180002006 **Time: 8/18/2020 11.32 AM**

Type	Amount	PayType	Amount	
Cash To Vault	-$258.00			
		Cash	-$258.00	
Total Type:	-$258.00	Total Paid:	-$258.00	**Status: Paid**
Transaction Count: 5 **Total Type:**	**$5,168.49**	**Total Paid:**	**$5,168.49**	

At this point in the workflow, the cashiering batch is balanced and closed. Batches are released into the workflow for ACH deposit and output to downstream systems. A graphical workflow monitor tracks the progress of batches through the system.

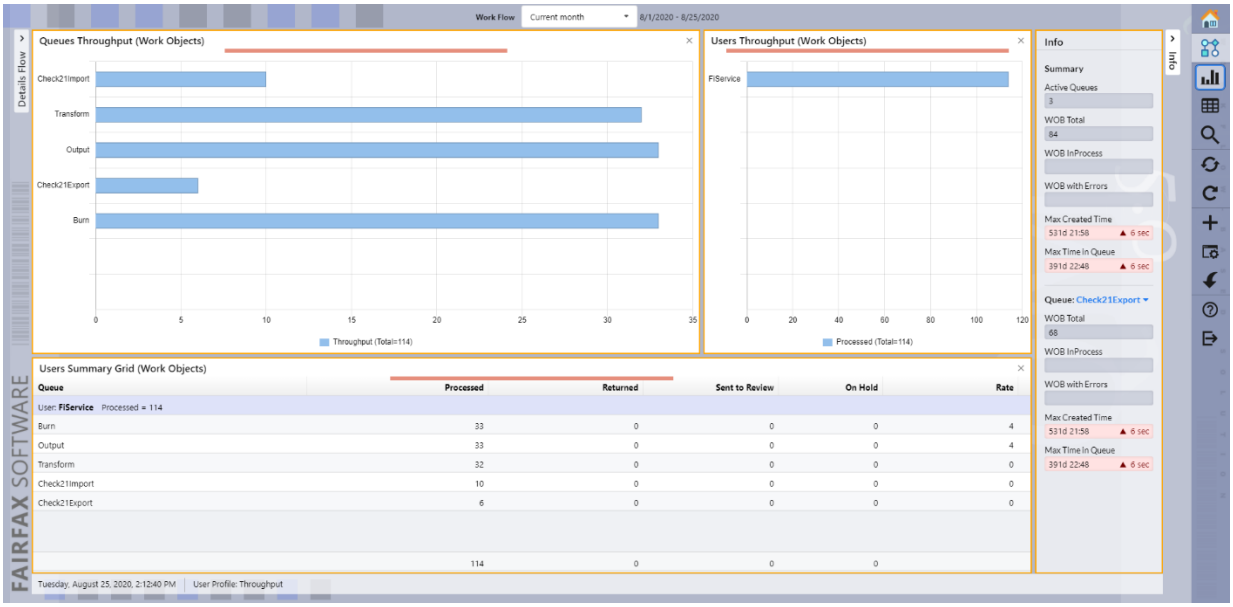


Figure 42 – Graphical Workflow Monitor

Quick Output

At this point in the workflow, all the data has been perfected and the transactions are awaiting output to downstream systems. *Quick* Output is a general-purpose output stage. It receives the results of the data entry and balancing stages and appends or stores the information in an output data file. After processing has been completed, there are a variety of options available to the Parish for output of the captured information (data and images). File creation and output consisting of various formats will be performed and multiple transmissions can be generated daily to maintain the system output.

Through *Quick* Modules' *Quick* Output module, data files will be created that can be transmitted to the designated endpoint(s) that the Parish requires. This can be one or many file-types from standard to highly custom. There is virtually no limit to the number and type of files that can be created, for as long as the file format can be specified, the interface can be developed.

ACH Processing

The solution includes ACH conversion of checks entered following the latest NACHA formats. ACH files submitted directly to Bank of America for deposit or to another agency as required.

System Monitoring and Reporting

The solution proposed offers a robust set of tools that allow the Parish to monitor the daily cashier production and archival databases of the designed solution. Fairfax Software recognizes the requirement to monitor the production systems continuously in order to achieve maximum productivity and address any cashiering bottlenecks. *Quick* Workflow Monitor will monitor performance on the centralized functions of the system.

Each cashiering location will have a management dashboard that reports the drawer status and the contents of each cash drawer in real-time.

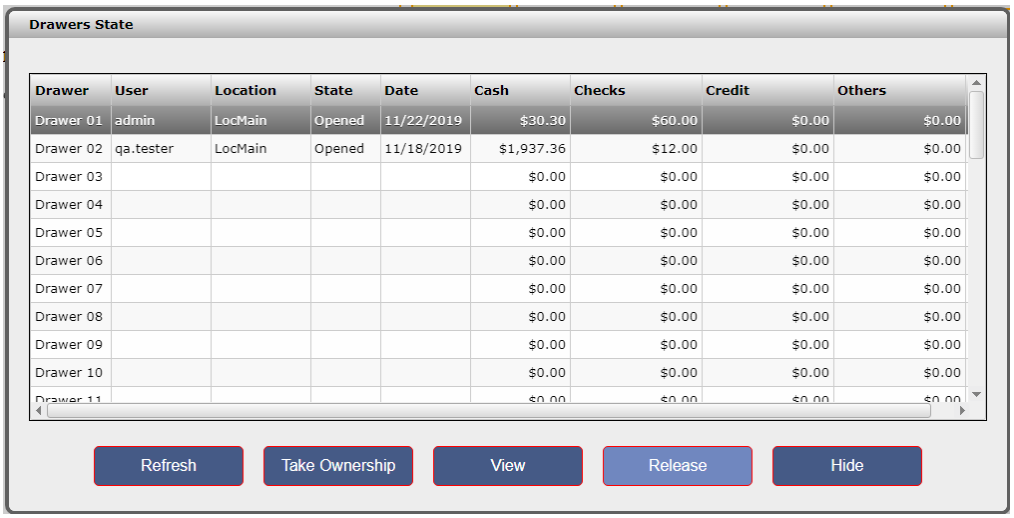


Figure 43 – Drawer Status

2. Plans for necessary training, where applicable. Information demonstrating an affirmative statement shall be required that the proposer has reviewed the scope of work, understands the nature thereof and is willing and capable of providing the services thereof.

Fairfax Software Response:

Fairfax Software meets this requirement.

Fairfax Software places a great deal of emphasis on training as an integral part of the installation process. Fairfax Software firmly believes that the system only produces the expected results when operated by well-trained personnel and that a brilliant solution will only show its illustrious result when operated by personnel familiar with its use and intricacies. This holds true for system administrators and users alike.

Fairfax Software provides all the training necessary to operate the proposed solution and knowledge transfer to allow the Parish to assume responsibility for maintenance and configuration of the solution in the future. All Fairfax Software instructors are experienced in the field of system training and have conducted courses on similar systems in the past at dozens of other government agencies.

Training is one of the hallmarks of our services, and as such, we can't over emphasize the importance of the training aspects of our solution. In addition to the formal hands-on training, we stress the importance of other types of knowledge transfer like on-the-job training, mentoring, and job shadowing. Training is provided near the rollout of each phase of the project.

Some of the techniques that we have successfully used for ensuring that a workforce is fully trained, proficient, and certified on all aspects of the system are:

- **Employing a more Consultative approach:** We will work with the Parish's project staff in bridging any gap at project inception between our respective backgrounds, knowledge of technology, practices and methods. Through our interactive work sessions, we will illustrate to the Parish staff members best practice and lessons learned. We cite real life examples that we acquired from other state department experiences. We listen openly to alternatives, and, in many cases, we adopt and mold our software to the preferred method. In instances, we propose other methods for doing things, and illustrate how and where these methods have been proven to be right and have saved their adopters time and money.
- **Subject matter expertise:** Dedicating subject matter experts in IT, interfaces, and business rules at various times of the project lifecycle has helped ensure passing of the appropriate knowledge to our technical and business staff, and in turn will result in accurate data being analyzed, captured, and passed.
- **Buddy approach to training:** We at Fairfax Software have long understood that any system is only as good as the personnel operating it. A well-trained operation team is essential. For that, we have paired team members from different government agencies with Fairfax Software team members, in order to have a way to gain familiarity with the operational environment and have knowledge transferred as part of the learning process.
- **Job shadowing with incumbent personnel:** In many instances, we have experienced shadowing the staff members at several government agencies. For there is no better way to understand the plight and the issues on hand as well as a job shadowing exercise.

As a standard and systematic part of its training offering, Fairfax Software offers integral end-to-end training to the following system personnel and staff members in the local government agency site:

- **Operators:** Operator training includes methods of logging in, system initiation, and logging off, and day-to-day operations and other relevant information necessary for the proper operation of the system.
- **Supervisors:** Supervisor training includes operator-level training, high-level system overview, and training of the supervisory tools available, including status, reporting and monitoring tools.
- **System Administrators:** Administrator training includes system start up and shut down, system recovery, system status, and all routine daily maintenance requirements.
- **System Support:** System support training will cover operational aspects of the scanning equipment, including use of systems software and any application software developed for, or provided under, this contract.
- **Management Overview**: Management Overview Training provides an extensive overview of all systems, transactions and the functionality of the entire system.
- **Train-the-Trainer:** Fairfax Software believes strongly in providing Train-the-Trainer instruction in both operational and technical support training for as many Parish personnel as required.

We propose a methodology for training that will include step-by-step procedures and directions in the use of the proposed solution through all the activities supported by the solution. One that combines both formal and on-the-job training processes, using the following four-tiered approach:

- **Mentoring:** Throughout the development period and while the system is being prepared and tested, our staff offers our customer users continuous support and mentoring through the infusion of ideas and practical experience between the teams.
- **Formal training in a classroom setting:** This is a formal session with projected presentations and handouts. These sessions are interactive with the audience and have proven to be effective in imparting the theory prior to the practical sessions.
- **On-the-Job training:** This is one of the most effective ways of transferring the knowledge that is needed to run the system and having it retained for the longest period of time. This method has proven that the knowledge imparted this way has the greatest effectiveness in terms of application of the knowledge and retention of the information by the target audience.
- **Post-production:** During this period, a dedicated resource will be focused on assisting the Parish in the live production environment. This combination of mentoring, on-the-job training, and teamwork assists our customer personnel to handle the system's operations from that point on. We find this period of support to be important to the success of our customers in terms of effectively operating the system.

We believe that this combined methodology will yield trained, qualified Parish staff to show the value of the system and take advantage of its potential. A well-trained user community is also able to reap benefits from the system to the fullest extent. This methodology is proven in that it has been used successfully on other projects similar in scope and nature to this Parish project and at dozens of other government agencies throughout the United States and Canada.

TAB D – PROPOSER QUALIFICATIONS AND EXPERIENCE

History and background of Proposer, including but not limited to status with related services to government entities existing customer satisfaction, demonstrated volume of merchants, etc.

Fairfax Software Response:

Qualifications and Experience
Our solution is built on over twenty-seven (27) years of experience delivering award winning solutions that are currently processing billions of dollars and millions of transactions per day for government departments across the United States, Canada, and New Zealand. We focus on government accounts and have installations in over forty-six (46) government agencies, including many city and local governments.

As a leading provider of proven remittance, on-line payment, cashiering, forms, and software solutions worldwide, Fairfax Software is highly qualified to deliver the proposed solution to meet all of the Jefferson Parish requirements. Our expertise centered on payment processing has been attained from over twenty-seven (27) years of business excellence and delivering highly successful implementations that meet and exceed our client's requirements.

Our extensive corporate experience is exhibited in the large number of clients which continue to grow and outpace our competition. The listing provided below of just a few of our many clients provides the example of our past experiences in implementing solutions which are relied upon for everyday use.

Local (City/County) Revenue Departments: City of Virginia Beach, City of Philadelphia, City of Chicago, District of Columbia, County of Hawaii, Gwinnett County, GA, Jefferson Parish, Los Angeles County, Kern County, CA.

State Revenue Departments: Alabama, Colorado, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Massachusetts, Mississippi, Montana, New Hampshire, New Jersey, Oklahoma, Ohio, Oregon, Rhode Island, West Virginia, West Virginia State Treasury Office (STO).

Department of Motor Vehicles: California, Texas, Florida, Ohio, Virginia.

Child Support Departments: Montana Child Support, South Dakota Child Support.

Labor Departments: Colorado, Georgia, Missouri, Tennessee, Texas.

Insurance and Healthcare: New York Life, Kaiser Permanente, BCBS of Rhode Island, New York State Health & Hospitals, Aetna, Humana, Premera Blue Cross.

International: New Zealand Ministry of Innovation and Business, Tangerine Bank, Province of Ontario Ministry of Finance, Province of Saskatchewan Ministry of Finance.

Non-Profit: Food for the Poor.

Order Entry: Checks in the Mail, Winston Brands.

Each of the above accounts utilizes and relies daily on Fairfax Software's solutions each and every day. The reliability of the solution related modules and their ability to address a wide range of unique processing requirements is exhibited in the above list of clients who process billions of dollars of transactions daily on our system offerings.

1.4 Proposer Minimum Requirements

The proposer shall:

A. Be a firm or corporation regularly engaged in the acceptance and processing of debit/credit cards and other forms of electronic payments, providing on-line reporting services and/or collection agent.

Fairfax Software Response:

Fairfax Software is a solution provider engaged in processing debit/credit cards and other forms of electronic payments, as well as point of sale (over the counter) payments and paper-based payments. Inclusive to the processing of all forms of payments, Fairfax Software provides on-line reporting that consolidates these various means of acceptance of payments for a combined, comprehensive reporting.

B. Demonstrate to the satisfaction of the Parish that the Proposer has adequate financial resources, experienced personnel, and experience in processing debit/credit cards and other forms of electronic payments.

Fairfax Software Response:

Fairfax Software has the financial means, as well as the experience and background to provide the services to the Parish for the purposes of processing debit/credit cards and other forms of electronic payments. These capabilities are exhibited through our Corporate Financial Statements which are included herein to this RFP response; our staff resumes submitted herein, as well as the number of current clients who rely on Fairfax Software each day for processing payments.

C. Provide documentation to support the qualifications criteria as part of the RFP.

Fairfax Software Response:

Fairfax Software provided its qualifications above in “TAB D – Proposer Qualifications and Experience”, and in “TAB F – Project Schedule” for our project methodology and resumes for the support staff for this project.

D. Be able to provide a cost-effective solution for merchant services.

Fairfax Software Response:

The Fairfax Software solution includes Visa, MasterCard, Discover, and American Express card processing through Govolution, providing all merchant services for the project using Point to Point Encrypted Devices (P2PE) for card present and digital wallet transactions. Please see TAB C – Technical Solution for more details.

E. Provide a single point of contact for customer relations.

Fairfax Software Response:

The Parish's single point of contact for customer relations is:

Michael Minter
VP, Sales and Marketing
Office: 703-802-1220 x103
Mobile: 214-384-3174
Email: mminter@fairfaxsoftware.com

F. Provide real time web-based reporting of transactions by department and/or location.

Fairfax Software Response:

The proposed solution is Web-based for easy deployment and support and provides the Parish with a web interface to take payments, manage configuration and run daily reports. The system's robust and comprehensive reporting is based on Microsoft SQL Server Reporting Services (SSRS) and provides full logging (verbose and summary) and full audit tracking reporting through standard and customized reports.

All reports can be exported in common formats including but not limited to, Microsoft Excel, Microsoft Word, Adobe PDF, Comma Separated Values (CSV), Extensible Markup Language (XML), fixed field text (TXT), JavaScript Object Notation (JSON).

Reports can be run on a specific date or range of dates. Reports can be viewed or downloaded in a variety of formats including PDF, Word, and Excel. The Parish has control over all system reports. Standard reports include:

- Accounts in Collections
- Aged Receivables Report
- Audit Events
- Collections Report
- Credit Memos applied to Open Invoices
- Credit Memo Raised
- Delinquent Accounts
- Deposit Reports
- Overpayments
- Revenue Received
- Revenue Report
- Underpayments
- Underpayments and Overpayments

G. Provide immediate and direct deposit of all payments made by a customer, into a designated Parish bank account through a Parish-approved banking partner. At no time would the payments flow through a Contractor's bank account.

Fairfax Software Response:

The proposed solution allows direct deposit of all payments into any designated Parish bank account. This process is performed immediately upon clearing of the payment transaction and at no time will the payments flow through a Fairfax Software bank account.

H. Be PCI compliant.

Fairfax Software Response:

As part of our PCI Compliance and SOC2 audits, all our software is audited by an outside and independent specialized security firm for vulnerabilities. This process takes place every year and is very thorough in nature. This entity attempts to examine every aspect of our software development life cycle and attempts to penetrate our system looking for vulnerabilities. This outside entity publishes a report every year describing in detail the analysis and penetration processes performed and the exact outcome. Any potential vulnerabilities, whether rated high, medium and low are tracked and remediated.

All data processed by Fairfax Software solutions are encrypted to the highest level of encryption (256-bit), both in transit and at rest.

In addition, our software has been certified to comply with all the following security guidelines:

- FIPS 140-2
- IRS Publication 1075
- NIST SP 800-53
- Section 508
- WCAG
- PCI-DSS
- SOC2 Type 2
- DISA STIG

Lastly, Fairfax Software proudly produces software that is ADA-compliant and is certified to be used by people with disabilities.

The following tests are adhered to every year:

1. **SOC 2**: SOC 2 based on the criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria). The description is intended to provide report users with information about Fairfax Software's systems that may be useful when assessing the risks arising from interactions with Fairfax Software's system, particularly information about system controls that Fairfax Software has designed, implemented, and operated to provide reasonable assurance that the Company's service commitments and system requirements were achieved

based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

2. **PCI**: In accordance with PCI DSS v3.2.1, Revision 1.0 ("ROC Reporting Template"), Fairfax Software completes an annual PCI audit using the mandatory template for Qualified Security Assessors (QSAs) completing a Report on Compliance (ROC) for assessments against the PCI DSS Requirements and Security Assessment Procedures v3.2.1.
3. **Additional Laws and Regulations**: Fairfax Software's software and service offerings are also subject to the security, availability, processing integrity, confidentiality, and privacy requirements (as amended), including relevant regulations, as well as state privacy security laws and regulations.

I. Provide training as necessary to Parish Employees

Fairfax Software Response:

Fairfax Software places a great deal of emphasis on training, because we believe that the system will only produce the expected results when operated and administered by well-trained personnel:

- **Operators**: Operator training includes methods of logging in, system initiation, and logging off, and a day-to-day operation including research, reconciliation, and customer service functions.
- **Supervisors/Management**: Supervisor training includes operator-level training, high-level system overview, and training of the supervisory tools available, including dashboard status, reporting and monitoring tools.
- **Technical and System Support**: System technical and support training will cover operational aspects of the systems software and any software provided under this contract. This training will also include configuration and setup of System Templates and security settings
- **Train-the-Trainer**: Fairfax Software believes strongly in providing Train-the-Trainer instruction in both operational and technical support training for as many Parish personnel as required.

We propose a methodology for training that will include a step-by-step procedures and directions in the use of the proposed system through all the activities supported by the solution. One that combines both formal and on-the-job training processes, using the following four-tiered approach:

1. **Mentoring:** Throughout the development period and while the system is being prepared and tested, the resident on-site staff will offer continuous support and mentoring through the infusion of ideas and practical experience between the teams.
2. **Formal training in a classroom setting:** This is a formal session with projected presentations and handouts. These sessions are interactive with the audience and have proven to be effective in imparting the theory prior to the practical sessions.
3. **On-the-Job training**: This is one of the most effective ways of transferring the knowledge that is needed to run the system and having it retained for the longest period of time. This method has proven that the knowledge imparted this way has the greatest effectiveness in terms of application of the knowledge and retention of the information by the target audience.
4. **Post-production:** During this period, our on-site resource will be focused on mentoring in the live production environment. This combination of mentoring, on-the-job training, and teamwork will assist Parish personnel to handle the systems operations from that point on. We find this period of support to be important to the success of our customers in terms of effectively operating the system.

We believe that this methodology will yield trained, qualified Parish staff to show the value of the system, and take advantage of its potential. A well-trained user community is also able to reap benefits from the system to the fullest extent. This methodology is proven, and we have used it successfully on other projects. Many of our customers have given excellent feedback with regard to the effectiveness and longevity of the knowledge imparted.

In order to improve our training methods and techniques, we welcome the Parish's comments. At the end of each training session, Fairfax Software trainers will submit comment cards to the attendees in order to solicit feedback. This information and feedback are monitored by our Project Manager and Fairfax Software uses them as input to a process of continuous improvement. We encourage the Parish to make suggestions for improvement, and to propose other training techniques.

The following conditions typically govern the training environment:

- Scheduling of courses will be subject to mutual agreement between Fairfax Software and the Parish.
- Training will focus on the system on-hand (i.e., how the system works and how it goes about its operations) and not on basic concepts such as MS-Windows.
- All trainees will be provided with appropriate manuals, text materials, and course outlines necessary for the specified training.
- Fairfax Software will develop and provide implementation plans and a training curriculum to the Parish project manager.
- Fairfax Software will develop, with the Parish, a troubleshooting manual and a user manual.
- Manuals will be made available to Parish personnel during the implementation and final copies will be provided as part of the Systems acceptance process. These manuals will be the appropriate manual for each class and for each class participant.

- Fairfax Software will prepare a comprehensive training plan and submit a written curriculum to the Parish project manager for approval two months prior to training.

J. Be able to work with other Jefferson Parish vendors to facilitate construction of API's or other mechanisms to allow payment systems, financial reporting, and billing systems to electronically communicate.

Fairfax Software Response:

Using web services API's, all applications that require payments can have access to all of the features and functions provided by *Quick* Payments without costly time-consuming development required to add features to each individual application.

TAB E – INNOVATIVE CONCEPTS

Present innovative concepts, if any, not discussed above for consideration.

Fairfax Software Response:

The Fairfax Software *Quick* Payments solution brings state-of-the art electronic payment services to *all* departments of the Parish utilizing Govolution for Merchant Services. Govolution, together with Fairfax Software, provides the most secure and consolidated payment processing solution available.

The most obvious and important innovative benefit of the Fairfax Software solution to the Parish is the consolidation of the existing *Quick* Modules based remittance processing system with the *Quick* payments system into one homogeneous solution featuring consolidated reporting front-end to back-end. This reconciliation is enterprise-wide and is performed all the way from the receivables into the Parish's bank account(s). This innovation cannot be minimized and is, in our opinion, everything else being equal, the most important innovative feature in a procurement of this nature. These two solutions are born from the same family of products and technologies and feed into the same common database under the hegemony of the same common workflow, and most importantly are designed and supported by the same reliable vendor which has been by the Parish's side steadfast for over fifteen years.

Other innovative aspects of our *Quick* Payments solution in of itself include:

Innovation for the Citizen

A citizen can register with the *Quick* Payments system and have a single self-service application to support all payment processes for every Parish department. This easy consistent approach makes the citizen feel at ease when doing business with the Parish. If the process is easy and consistent, a citizen is more likely to use the service again-and-again. All payment options are available to the user including popular digital wallet payment methods such as Apple Pay®, Google Pay®, and PayPal®. All of the features that citizens use in the private sector are available including scheduled payments, automatic payments, and payment plans using their PC, phone, or tablet. The future-proof design of *Quick* Payments allows new payment methods to be added to the system as they become available. Once added to *Quick* Payments, they are instantly available to all departments.

The user may select any combination of payment types to complete the transaction with a consistent experience across all Parish departments. The shopping cart feature allows multiple payments to be made with a single transaction. A citizen can pay their utility bill and a library fine in a single transaction. An automatic transaction receipt provides all transaction information including payment confirmation for each payment type used. An automatic email of the transaction receipt is sent to the citizen.

Benefits of *Quick* Payments for Citizens

- A common payment experience across all Parish departments
- A shopping cart allowing multiple services across departments to be paid by a single payment
- A payment can be made by a combination of payment types
- A customer can save their card information for future payments

- A customer can set up recurring automatic payments
- A customer can set up a scheduled future payment
- Automatic notifications via email and SMS Text
- Customer self-service features including researching payment history
    - An individual customer is restricted to their own activity
    - A business customer is restricted to all activity within the business
    - History can be downloaded in PDF™, Word™ and Excel™ formats
- A PDF of the receipt is emailed automatically reducing paper waste

Innovation for the Back Office

Quick Payments provides Parish accounting staff with the tools to work faster and smarter. Automatic reconciliation features automate many manual 'busy work' processes freeing up accounting staff to focus on higher priority tasks.

By consolidating the payment processes that today are provided by various vendors, the Parish can track all payments with a single SQL database. Consolidated reporting, output, and posting simplifies the tasks required to support multiple vendors.

Benefits of *Quick* Payments to the Parish

- A single Microsoft® SQL™ database manages all parish payments in a single secure encrypted and controlled environment
- Comprehensive reporting using Microsoft® SQL Server Reporting Services™
    - Transaction level reports
    - Department level reports
    - Parish level reports consolidating all departments
    - Audit Reports
    - Custom reports
- System Templates allow Parish technical staff to add new departments with point-and-click ease
    - All receipt and email formats are customized with templates that can be edited with Microsoft® Word™
    - All department-level parameters are selected with the mouse
        - Allowable payment types
          For example, one department may allow credit cards and e-checks, where another department will only allow credit cards.
        - Allow scheduled payments
        - Allow payment plans
        - Allow automatically recurring payments
        - Allow partial payments
        - Web Branding
        - Define user roles and responsibilities
- Automatic reconciliation all the way to the Parish bank account(s)
- Automatic generation of General Ledger Entries
    - Credit card and bank statements are automatically reconciled to the matching database record.

- Automatic chargebacks processing
    - Chargebacks are automatically linked to the original transaction
    - Recorded customer information identifies the customer for collection
- Well-defined web services APIs are provided.

TAB F – PROJECT SCHEDULE

Detailed schedule of implementation plan for pilot (if applicable) and full implementation. This schedule is to include implementation actions, timelines, responsible parties, etc.

Fairfax Software Response:

Jefferson Parish Payment Processing Services

ID	Task Name	Duration	Start	Finish	Pred	Resource Names
1	**Jefferson Parish Payment Processing Services**	**74 days**	**Tue 7/5/22**	**Fri 10/14/22**		
2	**Vendor Selection**	**11 days**	**Tue 7/5/22**	**Tue 7/19/22**		
3	Vendor Notification	1 day	Tue 7/5/22	Tue 7/5/22		Jefferson Parish
4	Contract Negotiations	10 days	Wed 7/6/22	Tue 7/19/22	3	Jefferson Parish
5	**Project Preparation**	**1 day**	**Wed 7/20/22**	**Wed 7/20/22**		
6	Project Preparation	1 day	Wed 7/20/22	Wed 7/20/22	4	Fairfax Software, Jefferson Parish
7	Contract Final	1 day	Wed 7/20/22	Wed 7/20/22	4	Jefferson Parish
8	Identify Core Project Team	1 day	Wed 7/20/22	Wed 7/20/22	4	Jefferson Parish
9	**Design Preparation Activities**	**3 days**	**Thu 7/21/22**	**Mon 7/25/22**		
10	Prepare Kick Off Agenda	1 day	Thu 7/21/22	Thu 7/21/22	7	Fairfax Software
11	Kick Off Meeting	1 day	Fri 7/22/22	Fri 7/22/22	10	Fairfax Software, Jefferson Parish
12	Complete Design Schedule	1 day	Mon 7/25/22	Mon 7/25/22	11	Fairfax Software, Jefferson Parish
13	Project Kick Off Complete	0 days	Mon 7/25/22	Mon 7/25/22	12	Fairfax Software, Jefferson Parish
14	**Client Preparation**	**25 days**	**Mon 7/25/22**	**Mon 8/29/22**		
15	Project Management Plan	3 days	Tue 7/26/22	Thu 7/28/22	12	Fairfax Software
16	Quality Management Plan	3 days	Tue 7/26/22	Thu 7/28/22	12	Fairfax Software
17	Staffing Plan	3 days	Tue 7/26/22	Mon 8/29/22	12	Fairfax Software
18	Change Management Plan	3 days	Tue 7/26/22	Thu 7/28/22	12	Fairfax Software
19	Client Preparation Complete	0 days	Mon 7/25/22	Mon 7/25/22	12	Fairfax Software
20	**Requirements and Design**	**12 days**	**Tue 7/26/22**	**Wed 8/10/22**		
21	**Design Phase**	**12 days**	**Tue 7/26/22**	**Wed 8/10/22**		
22	**Business Process Analysis/Requirements**	**1 day**	**Tue 7/26/22**	**Tue 7/26/22**		
23	Architectural Review with IT team, server requirements	1 day	Tue 7/26/22	Tue 7/26/22	19	Fairfax Software, Jefferson Parish
24	**Collect Business Requirements**	**11 days**	**Wed 7/27/22**	**Wed 8/10/22**		
25	Billing Requirements	5 days	Wed 7/27/22	Tue 8/2/22	23	Fairfax Software, Jefferson Parish
26	System Configurations	5 days	Wed 8/3/22	Tue 8/9/22	25	Fairfax Software, Jefferson Parish
27	Output Requirements	3 days	Wed 8/3/22	Fri 8/5/22	25	Fairfax Software, Jefferson Parish
28	Integration Requirements	3 days	Mon 8/8/22	Wed 8/10/22	27	
29	Reporting Requirements	2 days	Wed 7/27/22	Thu 7/28/22	23	Fairfax Software, Jefferson Parish
30	**Application Security - Active Directory and Database Security**	**2 days**	**Fri 7/29/22**	**Mon 8/1/22**		
31	Discuss Application Users and Functions, Groups	0.5 days	Fri 7/29/22	Fri 7/29/22	29	Fairfax Software, Jefferson Parish
32	Application Database Security	0.5 days	Fri 7/29/22	Fri 7/29/22	31	Fairfax Software, Jefferson Parish
33	Reporting Requirements	1 day	Mon 8/1/22	Mon 8/1/22	32	Fairfax Software, Jefferson Parish
34	**Design Document Preparation**	**7 days**	**Tue 8/2/22**	**Wed 8/10/22**		
35	Prepare Draft Design Document	3 days	Tue 8/2/22	Thu 8/4/22	33	Fairfax Software
36	Deliver Draft for Review	1 day	Fri 8/5/22	Fri 8/5/22	35	Fairfax Software
37	Design Review	1 day	Mon 8/8/22	Mon 8/8/22	36	Jefferson Parish
38	Update Design Document with Feedback	1 day	Tue 8/9/22	Tue 8/9/22	37	Fairfax Software
39	Deliver Final Design Document	1 day	Wed 8/10/22	Wed 8/10/22	38	Fairfax Software
40	Sign Off - Design Document Complete	0 days	Wed 8/10/22	Wed 8/10/22	39	Jefferson Parish

Jefferson Parish Payment Processing Services

ID	Task Name	Duration	Start	Finish	Pred	Resource Names
41	**Configuration/Build Phase**	**20 days**	**Thu 8/11/22**	**Wed 9/7/22**	**40**	
42	**Customization/User Exit Development**	**20 days**	**Thu 8/11/22**	**Wed 9/7/22**		
43	Input Rules and Configuration	20 days	Thu 8/11/22	Wed 9/7/22	20	Fairfax Software
44	Look ups - Customizations	20 days	Thu 8/11/22	Wed 9/7/22	20	Fairfax Software
45	Workflow configuration	20 days	Thu 8/11/22	Wed 9/7/22	20	Fairfax Software
46	Integration	20 days	Thu 8/11/22	Wed 9/7/22	20	Fairfax Software
47	Web services for multiple collection sources	20 days	Thu 8/11/22	Wed 9/7/22	20	Fairfax Software
48	**System Installation & Configuration**	**16 days**	**Thu 9/8/22**	**Thu 9/29/22**		
49	**System Configuration and Custom Code**	**16 days**	**Thu 9/8/22**	**Thu 9/29/22**		
50	**Servers and Storage Ready (VM and Physical)**	**12 days**	**Thu 9/8/22**	**Fri 9/23/22**		
51	Setup- Environment System Install	4 days	Thu 9/8/22	Tue 9/13/22	45	Fairfax Software
52	Database Design and Configuration	4 days	Wed 9/14/22	Mon 9/19/22	51	Fairfax Software
53	*Quick* Modules Service Modules	4 days	Wed 9/14/22	Mon 9/19/22	51	Fairfax Software
54	Desktop Applications	4 days	Tue 9/20/22	Fri 9/23/22	53	Fairfax Software
55	**Hardware Periphials Installation**	**4 days**	**Mon 9/26/22**	**Thu 9/29/22**		
56	Install 4 POS devices	4 days	Mon 9/26/22	Thu 9/29/22	54	Fairfax Software, Jefferson Parish
57	**Unit Testing**	**5 days**	**Mon 9/26/22**	**Fri 9/30/22**		
58	Review modular code	5 days	Mon 9/26/22	Fri 9/30/22	54	Fairfax Software
59	Test component modules to product specifications	5 days	Mon 9/26/22	Fri 9/30/22	54	Fairfax Software
60	Identify anomalies to product specifications	5 days	Mon 9/26/22	Fri 9/30/22	54	Fairfax Software
61	Modify code	5 days	Mon 9/26/22	Fri 9/30/22	54	Fairfax Software
62	Re-test modified code	5 days	Mon 9/26/22	Fri 9/30/22	54	Fairfax Software
63	**Integration Testing**	**5 days**	**Mon 10/3/22**	**Fri 10/7/22**		
64	Obtain Test Data and Confirm Data Exchange/interface	5 days	Mon 10/3/22	Fri 10/7/22	62	Fairfax Software, Jefferson Parish
65	Create Test Plan	5 days	Mon 10/3/22	Fri 10/7/22	58	Fairfax Software, Jefferson Parish
66	Create High Level Test Cases	5 days	Mon 10/3/22	Fri 10/7/22	58	Jefferson Parish
67	Create Manual Test Scripts	5 days	Mon 10/3/22	Fri 10/7/22	58	Jefferson Parish
68	Conduct testing and automated scripts	5 days	Mon 10/3/22	Fri 10/7/22	58	Jefferson Parish
69	Defect Management	5 days	Mon 10/3/22	Fri 10/7/22	58	Jefferson Parish
70	Create test summary report	2 days	Mon 10/3/22	Tue 10/4/22	62	Fairfax Software ,Jefferson Parish
71	**UAT Testing**	**8 days**	**Wed 10/5/22**	**Fri 10/14/22**		
72	UAT Testing	5 days	Wed 10/5/22	Tue 10/11/22	70	Jefferson Parish
73	Defect Management	5 days	Wed 10/5/22	Tue 10/11/22	70	Fairfax Software, Jefferson Parish
74	Volume/Stress Test	3 days	Wed 10/12/22	Fri 10/14/22	73	Fairfax Software, Jefferson Parish
75	Performance Testing	2 days	Wed 10/12/22	Thu 10/13/22	73	Fairfax Software, Jefferson Parish
76	Testing Complete / Ready for Production	1 day	Fri 10/14/22	Fri 10/14/22	75	Fairfax Software , Jefferson Parish
77	**Production/Final System Acceptance**	**1 day**	**Mon 10/17/22**	**Mon 10/17/22**		
78	Production Cutover/Deployment	1 day	Mon 10/17/22	Mon 10/17/22	76	Fairfax Software, Jefferson Parish
79	Go Live - Production	0 days	Mon 10/17/22	Mon 10/17/22	78	Fairfax Software, Jefferson Parish

Fairfax Software's project planning methodology is based on industry best practices and established standards derived from the PMI Institute's Project Management Body of Knowledge (PMBOK). We have adopted and deployed these strategies as part of our project development life cycle, and they have proven successful on projects similar in scope and nature to that of Parish.

Each project consists of initiating, planning, executing, controlling/monitoring, and closing phases to provide guidance to the process. Within each of these, specific tasks enacted upon by the Fairfax Software team or provided deliverables ensure a defined approach to the execution of the project.

Regardless of size of the project or phases, the methods used by Fairfax Software team allow proper management, planning, and execution to the overall goals and project implementation.

The overall approach is illustrated below.

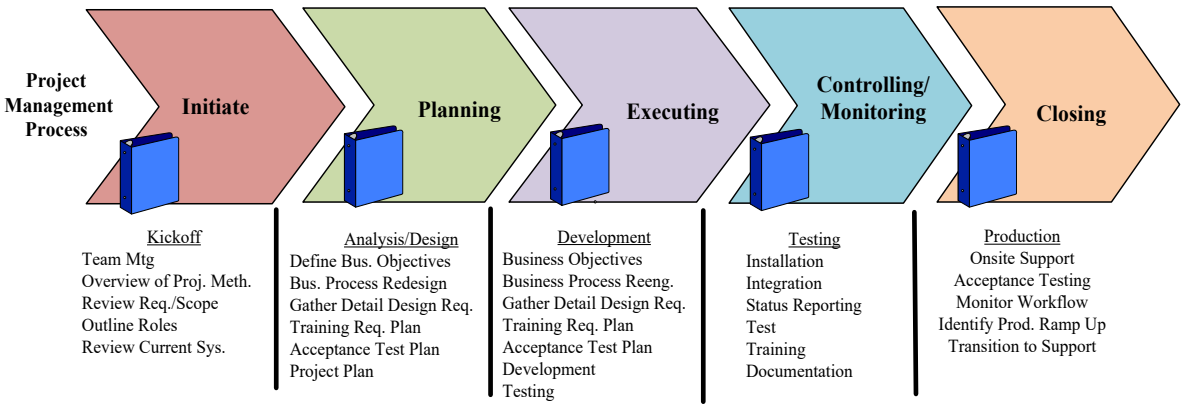


Figure 44 – Project Management Process

Fairfax Software will implement the project through deployment and use of a number of strategies that have made us successful in the past. These strategies are stated as follows:

1. Timely execution through measured project deliverables
2. Timely and meaningful project reporting and communication
3. Quality assurance and risk mitigation
4. Adherence to State and Corporate standards and processes
5. Implementation of a thorough test strategy in multiple phases
6. Application of internal quality control monitoring of project deliverables and project status
7. Application of the appropriate support structure
8. Establishment of a base line for our system from which to measure progress

These are central to our overall corporate delivery methodology and are documented and understood on a corporate-wide basis.

Timely Execution through Measured Project Deliverables

Fairfax Software will produce a number of project deliverables as progress is being made on the project and in strict accordance with milestones set forth and agreed upon as part of the System Detail Design and Master Project Plan.

We classify these deliverables by type:

Project Management Deliverables:

- Project Plan (Updated weekly throughout project)
- Weekly Progress Status Reports, including tasks accomplished/planned, tracking of issues with resolution, and risk register.
- Training Plan

- Change Control Plan
- Acceptance Test Plan
- Risk Mitigation Plan

Technical Deliverables:

- Detailed System Design and Functional Specifications (including interfaces)
- User Library/Exit Routines Functional Description
- System Documentation

System Deliverables:

- Training Material Deliverable
- End User Documentation
- System Test Plan
- Final Project Report

These deliverables will be a final and integral part of the project and will be owned by Parish. Should Parish require changes to the solution at a later time, they will have documentation and system descriptions to enable them to perform these changes readily and without necessarily requiring the assistance of our technical teams.

Project Management Deliverables

Project Plan

Soon after contract award and following the detailed Joint Application Design (JAD) sessions with the Parish business and technical staff, our Project Manager will provide an updated project plan. This update will take into account all the elements of the RFP and system design and implementation discussions as part of the JAD sessions that were reached during the design session between the Fairfax Software team and the Parish team.

Weekly Progress Status Reports

Fairfax Software Project Manager will have the responsibility of producing a weekly status report, outlining the latest developments on the project and how the team is able to meet the schedule. Weekly status reports will include requirements from all Project Management Plans. The schedule will be attached to the status report and the specific milestones highlighted as they are being met.

Training Plan

Fairfax Software Training Manager in conjunction with Parish Operation staff will prepare a custom training plan to suit the specific project requirements. This training will consist of training for:

- Operation staff
- Supervisor and Management (as needed) staff
- Technical staff (consisting of system configuration and infrastructure layout/build)

Change Control Plan

A change control plan that covers all aspects of the change control process. This deliverable may also be updated or more specifically tailored to meet the specific project requirements.

Risk Mitigation Plan

A risk mitigation plan that shows the methodology that we employ to manage and mitigate risk at the corporate level as well as at the project level. This deliverable may also be updated or more specifically tailored to meet the project requirements, as the specific risk assessment for this project will be evaluated with the knowledge, both a-priori (pre-award) and a-posteriori (post JAD sessions) of the project conditions and Parish expectations.

Technical Deliverables

Detailed System Design and Functional Specifications

At the inception of the project, Fairfax Software Project Manager will hold joint technical discussion sessions with various representatives of the Parish technical and user communities. These sessions will be detail oriented in nature, and will involve the project development activities, to include, but not be limited to business process re-engineering; the data capture aspect of the system, check processing, system interfaces and the other facets of the system design and implementation.

Parish System Documentation

Fairfax Software will provide all system documentation to the Parish technical personnel (IT staff) and system administrators. The system documentation will consist of the following two document types:

- **Vendor Documentation**

  Fairfax Software defines vendor documentation as those manuals and other materials provided by the manufacturer relating to each manufacturer's individual hardware (if applicable) and software product. All vendor documentation provided by Fairfax Software is in compliance with version levels and current operating procedures used to install and maintain the system environment.

- **System Documentation**

  Fairfax Software defines system documentation as the manuals, specifications, and guides prepared as part of the system development life cycle. The systems documentation ensures that Parish employees have the information needed to operate the equipment, troubleshoot at a basic or detailed level, and maintain the database.

System Deliverables

Training Material Deliverable

Prior to training commencement, the Fairfax Software Training Manager will prepare a set of outlines and handouts that will accompany the trainer during the training sessions. These illustrative elements include “cheat sheets,” small notes, and other visual material as necessary for training to be conducted in an efficient and practical manner.

End User Documentation

End-user system procedures prepared by Fairfax Software give step-by-step instructions that allow the end-user to accomplish a wide variety of tasks without the need for assistance. These procedures cover entry of data, specification of outputs, and operation of information system equipment such as scanners, workstations, and other relevant aspects of the proposed solution.

System Test Plan

Following the JAD sessions with Parish and the technical communities at the Parish site, Fairfax Software Project Manager will provide a detailed system test plan that will include the following elements at a minimum:

- Unit testing
- Regression testing
- Stress testing
- System testing
- Acceptance testing
- Test scripts

Final Project Report

At the end of the project development and implementation stage, Fairfax Software Project Manager will provide a final project report with the lessons learned.

Timely and Meaningful Project Reporting and Communication

Fairfax Software maintains open lines of communication among Fairfax Software team members on the one hand and with the Parish team on the other. These open lines of communication are used with Parish from project inception to completion. The same principles continue to apply beyond project completion, when the project transitions into maintenance mode.

The communication vehicles between Fairfax Software and the Parish staff, primarily the Parish Project Manager will be:

Team meetings

From the inception of the project, there will be regular meetings between the Project Manager and Parish staff. These meetings will be initially held two or three times a week or more depending upon the need. As the project matures and the development progresses, team meetings can be held weekly. Team meetings ensure that all issues and topics surrounding the project are covered and understood openly. Our objective is to foster a team environment, with an overall “can do” attitude, that infuses enthusiasm and open communication.

Weekly status reports

The Project Manager will produce a weekly status report, outlining the latest developments in the project and how the team will comply with the schedule. Weekly status reports will include requirements from the Project Management Plans. Such reporting will be attached to the status report and the specific milestones highlighted as they are being met.

Weekly status meetings

The Fairfax Software Project Manager will, with key members of the Fairfax Software implementation team, conduct a weekly status meeting with the Parish technical and managerial staff, particularly the Parish Project Manager. During these meetings, the weekly status report will be discussed in detail, and the issues surrounding it explored and analyzed.

Change Request

Fairfax Software is firmly committed to meeting the requirements stated by the Parish. No exceptions

have been taken, and there will not be exceptions made. Hence, we do not anticipate any changes to the project in scope or nature arising from Fairfax Software. However, we will still abide by the required protocol, should a change request arise or be needed. The Fairfax Software Project Manager will submit project change requests, to the Parish designated Project Manager. The Parish Project Manager will review and analyze project change requests and make a recommendation to Fairfax Software Project Manager. No changes will be made without the written approval of the Parish. The Parish Project Manager will receive and evaluate vendor deliverables from the vendor then respond to the Fairfax Software Project Manager with notification on the evaluation.

Significant reviews or meetings:

We suggest the following scheduled meetings.

- Kick-off meeting
- Weekly status meetings
- Constant interaction as a team
- Change request handling meetings

In addition, our Project Manager and Fairfax Software technical architects and specialists will be available to meet on an ad hoc basis if needed to meet certain specific requirements that were not met during regular meetings.

Fairfax Software has put together an experienced team of professionals with a high degree of business and technical qualifications and subject matter expertise to implement the proposed system. We align our teams with the tasks at hand. The project team shown herein exhibits the background and experience of performing similar projects to the Parish's project. Fairfax Software will work diligently with the Parish throughout the project to ensure all tasks are met in a timely fashion and to their satisfaction.

Our approach consists of empowering our Project Manager to be the Parish's best advocate and to make decisions that favor the project. We will also back our Project Manager with a highly qualified Business Analyst who is considered a subject matter expert. Our veteran developers all hold advanced computer science degrees and stand ready to implement any special requirements enunciated by the project's Business Analyst, approved by the Project Manager, and sanctioned by the Parish. Our Quality Assurance Director reports directly to the company's ownership and manages a team that consistently tests and presents its findings independently of the project team. These layers of expertise ensure our products are professionally designed, implemented and supported, with our customers' business requirements at the center of each decision made.

Please see our project team resumes below.

Jeff Allan

Team Position – Project Manager

Summary – 8+ years at Fairfax Software as Project Manager, managing successfully installed mission-critical financial processing applications for several state and local governments and insurance companies. Prolific experience in converting customer requirements into successful end-to-end cashiering and online solutions that tie into customers' legacy and back-end systems. All managed projects are referenceable. All managed solutions are currently in production and are being used by their respective customers on a daily basis.

Industry Experience

- ✓ *Financial transaction processing*
- ✓ *Government solutions integration*
- ✓ *Cashiering system and peripherals*
- ✓ *Online payment portals*
- ✓ *Data capture and perfection solutions*
- ✓ *Fund acceptance and reconciliation*

Specialization

- ✓ *18+ years large mission-critical systems management*
- ✓ *8+ years with Fairfax Software solutions and methodologies*
- ✓ *Payment and cashiering solutions*
- ✓ *Effective and creative problem resolution*

Education – Bachelor of Science, Management Information Systems, University of South Florida – 2004

Qualifications –

- 18+ Years of professional experience in managing information technology projects specifically in the financial processing and intelligent process automation industries.
- Proven track record of successfully delivering client engagements across several verticals markets, to include state and local governments, life and health insurance, and financial institutions.
- Expertise in using analytical and technical skills to create solutions tailored to customer requirements, fostering close relationships with clients to implement best practices.
- Strong written and verbal communications skills at all levels of the organization for business as well as technical audiences.
- Experience managing multiple concurrent cross-functional teams to include disciplines from the technical as well as the user communities.
- Expertise in gathering customer requirements and synthesizing them into a software solution that makes for a more efficient and elegant processing eliminating unnecessary and repetitive steps.
- Expertise collaborating with stakeholders (including external and internal ones) to ensure that requirements are clear and that all stakeholders agree on the deliverables.
- Full life cycle development and planning of large mission-critical financial processing systems.
- Acute understanding of customer experience, identify, and generate new ideas and improve software development aim at fulfilling the mission of the customers.
- Google Project Management Certificate – completed August 2021.
- PMP Certification: Completed qualification process to sit for the test (estimated May 2022).
- US Navy Veteran.

Project Experience –

- **Connecticut Department of Revenue Services (CT DRS)**
  - Period of Performance: 2016 - 2019
  - Brief Project Description: Complete remittance and financial transaction processing system serving the tax base processing for the entire State of Connecticut. Project included the full automation of all tax data capture from all tax forms in Connecticut, check acceptance, full incoming mail tracking, and interface to the State of Connecticut backend and legacy systems and databases as well as direct interface to the State of Connecticut's banks.
  - Project Role: Project Manager for a large integration effort involving several CTDRS automation operations for data capture, cashiering, check21 processing for over 1,200 tax form types, several custom modules, form redesign efforts, database conversions, archived data lookups, and a complete overhaul of the State of Connecticut check processing and tax acceptance. System is currently in production with state users statewide.
- **County of Kern, California**
  - Period of Performance: 2019 - 2020
  - Brief Project Description: Complete cashiering, remittance, and document processing system to include financial transaction processing and data capture from various property and other tax documents. Reconciliation of all County revenue into the County bank account. Implementation of a cloud-based secure cashiering system and training of the County staff in multiple departments on the use of the system.
  - Project Role: Managed the creation, configuration, cloud installation, implementation, and testing of the full-fledged solution to include all interfaces to the County legacy and backend systems. Managed the creation of custom burn and output modules created based on business requirements.
- **New York Department of Motor Vehicles (NY DMV)**
  - Period of Performance: 2020 - 2022
  - Brief Project Description: Complete hosted remittance and financial processing solution for the DMV encompassing the entire state of New York, from document acceptance to processing, output, and reconciliation, to include interfaces to the State of New York legacy and backend systems to pull data on-demand. The solution includes processing in several remote sites and one central location.
  - Project Role: Managed full hardware and infrastructure integration, requirement gathering, software implementation, various interfaces to satisfy specific client and statutory business rules into a full-fledged secure AWS Cloud integration.
- **Kansas Department of Revenue (KS DOR)**
  - Period of Performance: 2021 - Present
  - Brief Project Description: Complete financial processing solution for the entire state of Kansas, to include automation of various processes in the data capture and check deposit from taxpayers in Kansas. The system included the full development and integration of a Digital Data Automation (Channel Modernization) solution and the improvement of various financial processing procedures.
  - Project Role: Managed all aspects of the solution to include system design, requirements gathering, software implementation, system interfaces to outside legacy Kansas systems, system fielding, and QA testing.

- **Delaware Department of Revenue (DE DOR)**
  - Period of Performance: 2015 – 2017, and 2019 - 2020
  - Brief Project Description: Complete remittance, forms data capture, and financial transaction acceptance and processing. The system serves the entire tax base of the State of Delaware. Project included the full automation of all tax data capture from ALL tax forms in Delaware to include payment processing.
  - Project Role: Managed the entire integration effort from specifications and design to final implementation and testing for completing the initial Go Live of the roll-out (2015 – 2016) – Version 5.3, and follow-on multiple upgrade efforts (2019 – 2020) into Version 5.6. Assisted DE DOR in achieving key strategic decision points to save time and labor and become more efficient at various automated tasks that were previously manual.
- **Montana Department of Public Health & Human Services (MT DPHHS)**
  - Period of Performance: 2019 - 2020
  - Brief Project Description: Complete processing of child support payments for the entire State of Montana, this project entailed the management of multiple payments for one recipient and single payment for multiple recipients, verifying fulfillment of payments across the state. Established with online solutions that tie into Montana's legacy and back-end systems, complete tracking of the payments from receipt into the state's banks was realized, along with reconciliation and classification of the receipts.
  - Project Role: Implemented Fairfax Software's project methodology in the management of a large mission-critical child support application. Managed customer expectations and implemented customer requirements within the solution to include several interfaces to the courthouses and the state legacy systems.
- **New York Life Insurance Company (NYL)**
  - Period of Performance: 2014 – 2015 (Implementation of Version 5.3), and 2020 – 2021 (Implementation of Version 5.7).
  - Brief Project Description: Original scope consists of a large solution to handle acceptance of life insurance premium payments and other pertinent documents. Second scope included a large upgrade and major expansion of the previous system functionality. System included backend storage and retrieval and fanning out of the data captured to over 2,000 users and case workers nationwide.
  - Project Role: Managed all aspects of the integration and implementation effort into NYL's operations including requirements gathering and system discovery, design, integration, implementation, and testing of the entire solution into the NYL environment. Managed the entire digital transformation and training of the NYL front-end and back-end users. Same consistent effort implementing Fairfax Software project methodology done twice, once for the initial system rollout and then an upgrade which included ample additional functionality.
- **Colorado Department of Labor and Employment (CDLE)**
  - Period of Performance: 2015
  - Brief Project Description: Complete end-to-end implementation of a wage and employee/employer data capture and financial payment item processing system to include financial data reconciliation, data capture and validation, and various interfaces to the State of Colorado employer and employee databases.
  - Project Role: Managed the implementation of a wage reporting system for collection of data along with remittances from various employer submitted financial, payroll, and benefit documents. This project included full real time acceptance and processing of data elements for CDLE.

- **Oklahoma Employment Security Commission (OK ESC)**
  - Period of Performance: 2014
  - Brief Project Description: Design and implementation of a wage and employee data capture and financial check processing system to include bank data reconciliation, data capture and validation, and various interfaces to the State of Oklahoma employer and employee databases.
  - Project Role: Managed every aspect of the implementation by interfacing with stakeholders and managing to their expectations. Managed the fielding of the solution within the ESC infrastructure and the interfaces to the various state databases. Managed the testing and integration of the solution and assisted the customer in the user acceptance testing of the solution and participated in the initial go-live period.
- **Premera Blue Cross Blue Shield (CBCS)**
  - Period of Performance: 2014 – 2016
  - Brief Project Description: Solution designed and implemented to handle the acceptance and processing of health insurance premium payments and other pertinent documents. The solution included innovative methods for improving the BCBS and workflow and streamlining the BCBS operations. The system included various interfaces to outside databases and lookup functions that helped consolidate many processing functions within one new solution.
  - Project Role: Managed all aspects of the solution development and integration from requirements gathering to final implementation, user training, and final project implementation checklist.

Fuchi Xiong

Team Position – Business Analyst

Project Role and Description of Role – 3+ years at Fairfax Software as a Business Analyst, successfully applying analytical and problem-solving skills to develop and integrate financial processing for mission-critical financial processing applications for several state and local governments. Highly effective capture and understanding of unique business rules and workflow processes essential to successful implementations. Extensive experience converting customer requirements into successful end-to-end financial processing solutions. All managed projects are referenceable. All managed solutions are currently in production and are being used by their respective customers on a daily basis.

Education – Bachelor of Science in Software Engineering, Florida Gulf Coast University – 2018

Industry Experience

- ✓ *Payment Processing*
- ✓ *Government Solutions Integrations*
- ✓ *Financial Transaction Processing*
- ✓ *Data Capture and Data Modeling*
- ✓ *Payment and cashiering solutions*

Specialization

- ✓ *3+ years with Fairfax Software solutions and methodologies*
- ✓ *Remittance acceptance and payments*
- ✓ *Effective and creative problem resolution*
- ✓ *Strong communication skills*

Qualifications -

- 3+ Years of professional experience in technology and supporting large software projects.
- Proven track record of successfully delivering client engagements across different industries that include, state and local governments, and life and health insurance
- Expertise in payment processing, information management, work flow and business process improvements to effect positive change through well-designed technical solutions.
- Expertise in using analytical and technical skills to create solutions tailored to customer requirements, fostering close relationships with clients to implement best practices.
- Highly efficient gathering of customer requirements and transforming them into a more efficient and refined software solution, eliminating unnecessary and repetitive steps.
- Extensive experiences developing and executing training programs, authoring UAT scripts, and providing IT support for new systems.
- Positive motivator and participant in team environment and works well on individual projects.
- Strong written and verbal communications skills at all levels of the organization for business as well as technical audiences.
- Expertise collaborating with stakeholders (including external and internal ones) to ensure that requirements are clear and that all stakeholders agree on the deliverables.
- Extensive experience with JIRA, Confluence, SharePoint, manual journal entries for accounting and reconciliation as well as various data analytics tools.
- Acute understanding of customer experience, identifying and generating new ideas and improving the software development aim of fulfilling the mission of the customers.

Project Experience –

- **Kansas Department of Revenue (KS DOR)**

- Period of Performance: 2021 - Present
- Brief Project Description: Financial processing solution for the entire state of Kansas. The system included the full development and integration of a Digital Data Automation (Channel Modernization) solution and the improvement of various financial processing procedures. Complete financial processing solution for the entire state of Kansas, to include automation of various processes in data capture and check deposit from taxpayers in Kansas.
- Project Role: Meeting the business requirements for the Kansas DOR, identified business processes and rules, codified requirements, documented processes, and configured and developed of all features and modules of the new *Quick* Modules 5.0 system.

- **Texas Department of Public Safety (TX DPS)**
  - Period of Performance: 2021 - Present
  - Brief Project Description: Comprehensive upgrade of the existing automated revenue processing software and hardware environment to a *Quick* Modules 5.0 solution and OPEX Falcon+ scanners, accommodating not only enhanced transaction capabilities and volumes for existing jobs, but also future expansion as the Department of Public Safety's business needs evolve.
  - Project Role: Successfully matched the stakeholders' and business liaisons' business requirements with the financial processing methodologies inherent in *Quick* Modules, updating design documents and collaborating with the project team to execute against these needs while maintaining business continuity for the Texas DPS.
- **New York Department of Motor Vehicles (NY DMV)**
  - Period of Performance: 2020 - 2022
  - Brief Project Description: Complete hosted remittance and financial processing solution for the DMV encompassing the entire state of New York, from document acceptance to processing, output, and reconciliation, including interfaces to the State of New York legacy and backend systems to pull data on demand. The solution includes processing in several remote sites and one central location.
  - Project Role: Managed, updated and maintained design documentation, developing validation rules in the environment, software configuration, such as Check21, and implementation from the legacy New York DMV system to the QM 5.0 system to meet their business requirements and assure the integrity of the system.
- **New York Life Insurance Company (NYL)**
  - Period of Performance:) 2020 – 2021
  - Brief Project Description: Original scope consists of a large solution to handle acceptance of life insurance premium payments and other pertinent documents. Second scope included a large upgrade and major expansion of the previous system functionality. System included backend storage and retrieval and fanning out of the data captured to over 2,000 users and case workers nationwide.
  - Project Role: Leading New York Life's integration and implementation effort from system discovery through unit testing of the entire solution in the NYL environment, assured that requirements were met and plans for expansion of business processes could be fully supported by this nation-wide application.
- **Oregon Department of Revenue**
  - Period of Performance: 2019 - 2020
  - Brief Project Description: Supplying an innovative approach to the state of Oregon's remittance and financial transaction processing system requirements and building upon the scanning platform already in place, the project team worked with business and technical

liaisons for the State to implement *Quick* Modules components to streamline their business processes. The project included data capture and validation, financial processing, and financial data reconciliation, assuring that our system will grow in lockstep with Oregon's growth and the resulting future business requirements.

- Project Role: In addition to maintaining and updating critical design documents, led the requirements gathering process to obtain an accurate view of the business drivers and needs of the state of Oregon for this project. Working closely with business counterparts and our project team, configured and implemented the entire solution to assure business continuity and set the groundwork for anticipated expanded functionality.

- **Delaware Department of Revenue**
  - Period of Performance: 2019-2020
  - Brief Project Description: Complete remittance, forms data capture, and financial transaction acceptance and processing. The system serves the entire tax base of the State of Delaware and the project included the full automation of all tax data capture from ALL tax forms in Delaware including payment processing. The upgrade of Delaware's systems to *Quick* Modules 5.0 and HTML5 version RB5 further expanded the security and technical capabilities required by the state of Delaware's Department of Revenue.
  - Project Role: As part of the *Quick* Modules 5.6 upgrade, managed creation and update of the design document and the development and configuration of *Quick* Modules for forms and validation rules that would meet the needs of their specific requirements. Assisted DE DOR in achieving key strategic decision points to save time and labor and become more efficient at various automated tasks that were previously manual.
- **West Virginia Department of Revenue:**
  - Period of Performance: 2018 – 2020
  - Brief Project Description: Providing a more efficient processing approach with a streamlined single-platform for all tax-types, our initial implementation of West Virginia DOR's financial and remittance processing system included a tightly integrated data capture and validation system for the entire state, connecting to backend and legacy systems and databases as well as direct interface to the State banks.
  - Project Role: Captured business processes, customer requirements, integration points, and transition methodologies required to implement the *Quick* Modules for West Virginia DOR. Complete update of design documents, development and configuration of the system modules to accommodate the complex forms and validation rules that would handle all the customer specific requirements.

John Ollis

Team Position – Project Engineer

Summary – 2+ years at Fairfax Software as Project Engineer, implementing and sustaining enterprise technical solutions, specifically in the financial processing and intelligent process automation industries. Full life-cycle discovery and planning of large, enterprise-essential systems with extensive experience converting customer requirements into successful end-to-end financial processing solutions. All managed projects are referenceable. All managed solutions are currently in production and are being used by their respective customers on a daily basis.

Industry Experience

- ✓ *Government solutions integration*
- ✓ *Financial transaction processing*
- ✓ *Data capture and remittance*
- ✓ *Internal and external cross-legacy integration*

Specialization

- ✓ *25+ years of professional experience supporting large software projects*
- ✓ *2+ years with Fairfax Software solutions and methodologies*
- ✓ *Effective Problem Resolution*
- ✓ *Strong communication skills*

Education – Bachelor's Degree in Math, Arkansas Tech University – 1996

Qualifications –

- 25+ years of professional experience in technology supporting large software projects.
- Proven track record of successfully delivering client engagements across different industry verticals, including state and local governments, insurance and financial institutions.
- Expertise in payment processing, document imaging, information management, work flow and business process improvements to realize change through well-designed technical solutions.
- Highly efficient gathering of customer requirements and transforming them into efficient and refined software solutions, eliminating unnecessary and repetitive steps.
- Expertise using analytical and technical skills to create solutions tailored to customer requirements, fostering close relationships with clients to implement best practices.
- Highly proficient architect of a variety of database storage, lookups, data capture and remittance solutions specific to a wide variety of customers' business rules.
- Compelling written and verbal communications skills to facilitate cooperation and successful project execution across the enterprise.
- Acute understanding of customer experience, identifying and generating new ideas and improving the software development aim of fulfilling the mission of the customers.

Project Experience –

- **New York Department of Motor Vehicles (NY DMV)**
  - Period of Performance: 2020 - 2022
  - Brief Project Description: Complete hosted remittance and financial processing solution for the DMV encompassing the entire state of New York, from document acceptance to processing, output, and reconciliation, to include interfaces to the State of New York legacy and backend systems to pull data on-demand. The solution includes processing in several remote sites and one central location.

- Project Role: Acting as the System Engineer for this project, collaborated with the project manager and the business analyst to fully understand the specific and customized requirements for building and updating the system components to meet New York DMV's expanded business needs.

- **New York Life Insurance Company (NYL)**
  - Period of Performance: 2020 – 2021
  - Brief Project Description: Original scope consists of a large solution to handle acceptance of life insurance premium payments and other pertinent documents. Second scope included a large upgrade and major expansion of the previous system functionality. System included backend storage and retrieval and fanning out of the data captured to over 2,000 users and case workers nationwide.
  - Project Role: As lead Project Engineer, managed all aspects of the documentation and installation effort, including design documents, workflow verification, backend and legacy systems integration and system testing each module within the New York Life environment.
- **Delaware Department of Revenue**
  - Period of Performance: 2019-2020
  - Brief Project Description: Complete remittance, forms data capture, and financial transaction acceptance and processing. The system serves the entire tax base of the State of Delaware and the project included the full automation of all tax data capture from ALL tax forms in Delaware including payment processing. The upgrade of Delaware's systems to *Quick* Modules 5.0 and HTML5 version RB5 further expanded the security and technical capabilities required by the state of Delaware's Department of Revenue.
  - Project Role: In addition to updating critical design documents to match the requirements set forth by Delaware DOR, developed and modified Windows services and web applications that would reflect all specifications put forth by the customer, followed by comprehensive testing, training and implementation.
- **West Virginia Department of Revenue:**
  - Period of Performance: 2018 - 2020
  - Brief Project Description: Already using *Quick* Moules 3.0 for a more efficient processing approach, and a streamlined, single platform for all tax types, West Virginia's Department of Revenue worked with Fairfax to upgrade their system to *Quick* Modules 5.0. Further expanding the financial processing capabilities with minimal impact to business continuity, the new system clears the way for new functionality and expanded business support for the State.
  - Project Role: Assuring the integrity of the system with respect to both business rules and system requirements, updated and maintained design documentation, developed validation rules in the environment and oversaw the migration from the earlier system to support the expanding fiscal responsibilities of the State of West Virginia.

TAB G – FINANCIAL PROFILE

Proposers are requested to submit documentation from the past three (3) years demonstrating proposer's financial stability. Documentation may include audited financial statements including balance sheets, income statements, documentation regarding retained earnings, assets, liabilities, etc. Such information should be included in the technical portion of the proposal submission and MUST NOT be included with the cost proposals and/or price schedules.

Fairfax Software Response:

Fairfax Software is providing the past three (3) years of our audited financial reports (2018, 2019, 2020). We are completing our 2021 audited reports and will provide those to the Parish upon completion.

Fairfax Software
Audit Reports
for
2018, 2019 and 2020

FAIRFAX IMAGING, INC. AND SUBSIDIARY

FINANCIAL STATEMENTS

WITH SUPPLEMENTARY INFORMATION

AND INDEPENDENT AUDITOR'S REPORT

DECEMBER 31, 2018 AND 2017

FAIRFAX IMAGING, INC AND SUBSIDIARY
CONSOLIDATED FINANCIAL STATEMENTS
DECEMBER 31, 2018 AND 2017

Contents

	Page
Independent Auditor's Report	1
Consolidated Balance Sheets	2-3
Consolidated Statement of Operations and Retained Earnings	4
Consolidated Statement of Cash Flows	5
Notes to the Consolidated Financial Statements	6-10
Consolidated Schedules of General and Administrative Expenses	11

OAKES, P.C.

3330 BOURBON STREET, SUITE 102
FREDERICKSBURG, VIRGINIA 22408
PHONE (540) 371-1300
FAX (540) 373-6172

INDEPENDENT AUDITOR'S REPORT

Board of Directors
Fairfax Imaging, Inc.
Tampa, Florida

We have audited the accompanying consolidated balance sheets of Fairfax Imaging, Inc. (an S Corporation) and subsidiary as of December 31, 2018 and 2017, and the related statements of operations and retained earnings and cash flows for the years then ended.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Subsidiary

We did not audit the financial statements for the years ended December 31, 2018 and 2017 of Fairfax Imaging (Vietnam) Co., Ltd, a consolidated subsidiary, whose statements reflect total assets and expenses constituting less than 1% of the related consolidated totals. The results of our audit expressed herein, insofar as it relates to the above is based solely upon the report of other auditors and accountants.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Fairfax Imaging, Inc. and subsidiary as of December 31, 2018 and 2017, and the results of its operations and its cash flows for the years then ended in conformity with generally accepted accounting principles in the United States of America.

Kevin T. Oakes, CPA

Fredericksburg, VA
July 23, 2019

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED BALANCE SHEETS
DECEMBER 31, 2018 AND 2017

ASSETS

	2018	2017
Current Assets		
Cash	$ 2,106,588	$ 1,910,781
Accounts Receivable, net	2,202,640	1,515,189
Unbilled A/R	-	453,249
Construction in Process	454,688	144,974
Prepaid Expenses	819,492	870,577
	5,583,408	4,894,770
Property and Equipment		
Furniture and Equipment	285,302	270,264
Less: Accumulated Depreciation	(248,568)	(224,314)
	36,734	45,950
Other Assets		
Deposits	14,537	15,187
Long Term Prepaid Expense	1,457	4,809
	15,994	19,996
Total Assets	$ 5,636,136	$ 4,960,716

See Independent Auditor's Report
See Accompanying Notes to Consolidated the Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED BALANCE SHEETS
DECEMBER 31, 2018 AND 2017

LIABILITIES AND STOCKHOLDERS' EQUITY

	2018	2017
Current Liabilities		
Accounts Payable	$ 1,263,760	$ 719,465
Accrued Expenses	406,864	378,069
Deferred Revenue	2,723,337	2,920,845
State Taxes Payable	33,463	33,463
	4,427,424	4,051,842
Total Liabilities	4,427,424	4,051,842
Stockholders' Equity		
Common stock, no par value, 20,000 shares authorized, issued and outstanding		
Additional paid-in capital	170,700	170,700
Equity Translation Adjustment	23,737	26,362
Retained Earnings	1,014,275	711,812
Total stockholders' equity	1,208,712	908,874
Total liabilities and stockholders' equity	$ 5,636,136	$ 4,960,716

See Independent Auditor's
See Accompanying Notes to Consolidated the Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED STATEMENTS OF OPERATIONS AND RETAINED EARNINGS
FOR THE YEARS ENDED DECEMBER 31, 2018 AND 2017

	2018	2017
Revenue		
Sales - Commercial and Government	$ 9,170,600	$ 8,181,590
Sales - Leased Equipment	178,211	191,986
Sales - Maintenance	7,508,715	7,191,245
Net Operating Revenue	16,857,526	15,564,821
Cost of Goods Sold	11,307,856	9,611,301
Gross Profit	5,549,670	5,953,520
Operating Expenses		
Depreciation and Amortization	24,254	4,898
Research and Development	1,020,629	1,336,184
General and Administrative	3,424,645	3,590,563
	4,469,528	4,931,645
Income from Operations	1,080,142	1,021,875
Other Income		
Interest Income	1,941	33
Interest Expense	-	(43,202)
Other Income	12,502	(18,860)
	14,443	(62,029)
Net Income Before Taxes	1,094,585	959,846
Provision for Taxes	23,340	28,528
Net Income	$ 1,071,245	$ 931,318
Retained Earnings		
Beginning of Year	711,812	602,161
Less: Distributions to Shareholders	(768,781)	(821,668)
End of Year	1,014,275	711,812

See Independent Auditor's Report
See Accompanying Notes to the Consolidated Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED STATEMENT OF CASH FLOWS
FOR THE YEARS ENDED DECEMBER 31, 2018 AND 2017

	2018	2017
Cash Flows from Operating Activities		
Net Income (Loss)	$ 1,071,245	$ 931,318
Reconciliation adjustments		
Depreciation and amortization	24,254	4,898
Bad Debt Expense	3,876	40,000
Changes in:		
Accounts receivable	(238,079)	2,677,213
Supplies	-	19,173
Deposits and other	55,087	84,804
Construction in Process	(309,714)	343,243
Accounts Payable and Accrued Expenses	573,090	(1,587,656)
Deferred Revenue	(197,508)	230,258
Deferred State Taxes Payable	-	29,006
Net cash provided by Operating Activities	982,251	2,772,257
Cash Flows from Investing Activities		
Net additions to property	(15,038)	(13,442)
Equity Translation Adjustment	(2,625)	34,055
Cash Flows from Financing Activities		
Line of Credit	-	(1,300,000)
Shareholder Distributions	(768,781)	(821,668)
Net (decrease) increase in Cash and Cash Equivalents	195,807	671,202
Cash and Cash Equivalents, beginning of the year	1,910,781	1,239,579
Cash and Cash Equivalents, end of the year	$ 2,106,588	$ 1,910,781

Supplementary Cash Flow Information

Cash paid during the year for:		
Interest	-	43,202
State & Canada income taxes	23,340	28,528

See Independent Auditor's Report
See Accompanying Notes to the Consolidated Financial Statements

1. Organization

Fairfax Imaging, Inc. (the Company) was incorporated on March 22, 1994, under the laws of the Commonwealth of Virginia, and is engaged as a developer of image scanning software and systems for commercial and governmental use. Fairfax Imaging (Vietnam) Co., Ltd., a 100% foreign-owned company was established by Fairfax Imaging, Inc. on December 21, 2006 with the investment certificate No. 411043000048 granted by the Ho Chi Minh City People's Committee. The operation period of Fairfax Imaging (Vietnam) Co., Ltd. is 20 years, starting from the date of the investment certificate.

2. Summary of Significant Accounting Policies

Basis of Accounting – The Company maintains its books under the accrual method of accounting in accordance with generally accepted accounting principles. The accrual basis of accounting provides that revenues and gains are recognized when earned and expenses and losses are recognized when incurred. Consolidated financial items are recorded at historical costs and often involve the utilization of estimates. Consequently, consolidated financial statement items do not necessarily represent current values.

Revenue and Cost Recognition – The Company enters into multiple deliverable arrangements which may include any combination of services to include sale of hardware to customization and implementation of software. A multiple deliverable arrangement is separated into more than one unit of accounting if all these criteria are met:

- The delivered item has value to the client on a stand-alone basis;
- There is no objective and reliable evidence of the fair value of the undelivered item; and
- Delivery is considered probable and is under the Company's control.

If these criteria are met for each element and there is no objective and reliable evidence of fair value for all units of accounting in an arrangement, the arrangement consideration is allocated to the separate units of accounting based on each unit's relative fair value.

The Company provides technical support to customers with maintenance contracts, on an as needed and if available basis. The Company recognizes customer support revenue, including support revenue that is bundled with product sales, ratably over the term of the contract period, which generally ranges from six months to one year. Revenues from services are recognized when the services are performed.

Revenue and Cost Recognition (continued)

Disputes arise in the normal course of the Company's business. The Company occasionally has disputes with customers for collection of funds because of events such as delays, changes in contract specifications, or questions of cost allowance or collection. Such disputes whether for claims or unapproved change orders, are recorded at the lesser of their estimated net realizable value or actual costs incurred when realization is probable and can be reliably estimated. Claims against the Company are recognized when loss is considered probable and the amount is reasonably determinable.

Depreciation – Depreciation is computed straight-line with computer equipment and software at 3 years while furniture and fixtures are at 7 years.

Research and Development – Research and Development costs are expensed as incurred. Costs incurred prior to establishment of technological feasibility are expensed as incurred and reflected as research and development expense in the accompanying consolidated statement of operations and retained earnings. For the year ended December 31, 2018, the Company did not capitalize any costs related to software development

Use of Estimates – The preparation of financial statements requires management to make estimates and assumptions that affect certain reported amounts and disclosures, including contract contingencies. Accordingly, actual results could differ from those estimates.

Cash and Cash Equivalents – The Company invests its cash solely in deposits with insured bank institutions. The total account balance periodically exceeds the Federal Deposit Insurance Corporation ("FDIC") insurance coverage. When this occurs there is a concentration of credit risk related to amounts on deposit in excess of FDIC insurance coverage. The risk is managed by maintaining all deposits in what management believes to be high quality institutions.

On November 9, 2010, the Federal Deposit Insurance Corporation (FDIC) issued a Final Rule implementing section 343 of the Dodd-Frank Wall Street Reform and Consumer Protection Act that provides for unlimited insurance coverage of non-interest bearing accounts. Beginning December 31, 2010 through December 31, 2012, all non-interest bearing accounts are fully insured, regardless of the balance of the account, at FDIC-insured institutions. Interest bearing accounts are insured up to a maximum deposit insurance amount of $250,000 per depositor per insured depository institutions. Beginning January 1, 2013, non-interest bearing accounts will no longer be insured separately from interest bearing accounts held at the same financial institution. All balances insured held at the same financial institution will be insured up to $250,000. As of December 31, 2018, cash balances exceeded FDIC limitations by $1,070,657.

Construction in Process – Construction in process consists of supplies delivered to customer locations and undergoing on-site installation.

Accounts Receivable – Accounts receivable is recorded at the amount the Company expects to collect on balances outstanding at year-end. Management closely monitors outstanding balances and write-offs throughout the year balances that have been deemed uncollectible. As of December 31, 2018, all accounts receivable were deemed collectible.

Advertising – Advertising costs are expensed as they are incurred. Advertising costs in 2018 and 2017 respectively were $0 and $476.

Income Taxes – The Company, with the consent of its shareholders, has elected to be treated as an S Corporation under the provisions of the Internal Revenue Code. In lieu of federal corporation income taxes, the shareholders of an S Corporation are taxed on their proportionate share of the Company's taxable income or losses for federal tax reporting purposes. The Company is subject to state taxes in thirty-two states as the Company operates in those states and those states assess tax on S Corporations. The Company is also subject to tax in Canada and Vietnam.

Effective January 1, 2009, the Company implemented the accounting guidance for uncertainty in income taxes using provisions of Financial Accounting Standards Board (FASB) ASC 740, *Income Taxes*. Using that guidance, tax positions initially need to be recognized in the consolidated financial statements when it is more likely than not the position will be sustained upon examination by the tax authorities.

As of December 31, 2018, the Company had no uncertain tax positions that qualify for either recognition or disclosure in the consolidated financial statements.

With few exceptions, the Company is no longer subject to US federal and state income tax examinations by tax authorities for years prior to 2015.

3. Investments

In 2007, Fairfax Imaging, Inc. established Fairfax Imaging (Vietnam) Co., Ltd., a 100% foreign owned Company. Fairfax Imaging (Vietnam) Co., Ltd. incurred a net loss in the amount of $316,225 for the year ended December 31, 2018 and a net loss in the amount of $278,946 for the year ended December 31, 2017. This investment has been accounted for under the consolidation method. Under the consolidation method, the financial statements of the investee are combined with those of the investor and intercompany amounts are eliminated. For tax purposes, Fairfax Imaging (Vietnam) Co., Ltd. is taxed as a separate entity under Vietnam tax laws.

4. Line of Credit

The Revolving Loan and Security Agreement with Valley National Bank, formerly USAmeribank, for short-term borrowings of $2,750,000 under two line of credit agreements, one for $2,000,000 and one for $750,000, which bear interest at the U.S. Prime Rate had no balance due as of December 31, 2018.

5. Commitments and Contingencies

In order to provide certain parts and equipment to fulfill applicable sales orders, the Company has entered into multiple contracts with suppliers for the purchase and manufacture of equipment. The Company is exposed to contingent liabilities regarding outstanding purchase orders with the suppliers. The amounts and limitations of any loss attributable to the Company would be conditioned upon the contract specifications governing the related purchase order.

Management estimates the maximum loss at December 31, 2018, assuming non-performance by the Company on all outstanding contracts, to be less than $50,000.

6. Economic Dependency

For the year ended December 31, 2018, management estimates that 25% of gross sales were received from commercial customers and 75% from the Canadian, Vietnamese, U.S. and State governments. No single customer accounted for more than 15% of sales.

7. Leases

The Company leases certain facilities and equipment under operating leases expiring at various dates. Rent expense for the office facilities under operating leases was $226,915 for 2018 and $213,687 for 2017. Future minimum rental obligations are as follows:

For the year ending December 31, 2019	$ 157,369
2020	162,431
2021	167,494
2022	172,557
2023	72,778
	$ 732,629

8. Employee Benefit Plan

The company maintains a 401(k) Profit Sharing Plan. The plan covers all employees of the Company. The Company makes a 4% mandatory safe harbor matching contribution to the plan annually. Total contribution expense was $146,715 for the year ended December 31, 2018 and $131,953 for the year ended December 31, 2017.

9. Income Taxes

As a result of its S election, the Company is not subject to federal income tax but is subject to income tax in certain states, Canada, and Vietnam. The Company has elected to file Composite State Income Tax Returns where applicable. Payments due with the composite returns are treated as distributions to shareholders. The provision for income taxes in 2018 was $23,340 and in 2017 was $28,528.

10. Related Party Transactions

Software Consultants of Tampa Bay, Inc was formed on October 29, 2018. The corporation is 100% owned by the shareholder of Fairfax Imaging, Inc. During 2018, invoices totaling $63,000 were issued to Fairfax Imaging, Inc. As of December 31, 2018, these amounts were payable to Software Consultants of Tampa Bay, Inc.

11. Change in Ownership

Saad Stephen Chahal as Trustee of the Saad Stephen Chahal Living Trust shall purchase from Tony F. Cristofano and Liz Y. Cristofano, co-trustees of the Tony Frank Cristofano Living Trust all of its shares of stock in Fairfax Imaging, Inc. for fair value, which the Court has determined to be $1,752,000. As agreed to by all parties, the effective date of the sale of the Tony Frank Cristofano Living Trust stock in Fairfax Imaging, Inc. shall be December 31, 2017. Thereby leaving the Saad Stephen Chahal Living Trust as the 100% owner of Fairfax Imaging, Inc.

12. Subsequent Events

In preparing the financial statements, the Company has evaluated events and transactions for potential recognition or disclosure through July 23, 2019, the date that the financial statements were available to be issued.

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED SCHEDULE OF GENERAL AND ADMINISTRATIVE EXPENSES
FOR THE YEARS ENDED DECEMBER 31, 2018 AND 2017

	2018	2017
Salaries	$ 765,072	$ 1,266,231
Bad Debt	3,876	40,000
Rent	226,915	213,687
Property, Sales, and Other Taxes	409,924	427,208
Advertising	-	476
Employee Benefits	161,039	153,143
Automobile	3,500	8,894
Bank Fees	17,860	7,739
Consulting	360,672	25,739
Contributions	-	340
Dues	45,072	43,489
Employee Training	2,490	2,704
Freight	-	93
Insurance	774,942	705,481
Licenses	1,109	7,751
Maintenance	2,469	819
Meals and Entertainment	15,392	29,003
Miscellaneous	3,618	26,629
Computer and Office Supplies	27,738	46,368
Payroll Processing	14,885	14,924
Postage	8,149	9,342
Printing	212	278
Professional Fees	258,805	222,136
Recruitment	11,816	3,448
Relocation	10,775	-
Seminars	1,494	-
Telephone	100,996	98,640
Temporary Assistance	3,948	48,718
Trade Show	6,008	24,340
Travel	185,869	162,943
Total	$ 3,424,645	$ 3,590,563

FAIRFAX IMAGING, INC. AND SUBSIDIARY

FINANCIAL STATEMENTS

WITH SUPPLEMENTARY INFORMATION

AND INDEPENDENT AUDITOR'S REPORT

DECEMBER 31, 2019 AND 2018

FAIRFAX IMAGING, INC AND SUBSIDIARY
CONSOLIDATED FINANCIAL STATEMENTS
DECEMBER 31, 2019 AND 2018

Contents

	Page
Independent Auditor's Report	1
Consolidated Balance Sheets	2-3
Consolidated Statement of Operations and Retained Earnings	4
Consolidated Statement of Cash Flows	5
Notes to the Consolidated Financial Statements	6-10
Consolidated Schedules of General and Administrative Expenses	11

OAKES, P.C.

3330 BOURBON STREET, SUITE 102
FREDERICKSBURG, VIRGINIA 22408
PHONE (540) 371-1300
FAX (540) 373-6172

INDEPENDENT AUDITOR'S REPORT

Board of Directors
Fairfax Imaging, Inc.
Tampa, Florida

We have audited the accompanying consolidated balance sheets of Fairfax Imaging, Inc. (an S Corporation) and subsidiary as of December 31, 2019 and 2018, and the related statements of operations and retained earnings and cash flows for the years then ended.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Subsidiary

We did not audit the financial statements for the years ended December 31, 2019 and 2018 of Fairfax Imaging (Vietnam) Co., Ltd, a consolidated subsidiary, whose statements reflect total assets and expenses constituting less than 1% of the related consolidated totals. The results of our audit expressed herein, insofar as it relates to the above is based solely upon the report of other auditors and accountants.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Fairfax Imaging, Inc. and subsidiary as of December 31, 2019 and 2018, and the results of its operations and its cash flows for the years then ended in conformity with generally accepted accounting principles in the United States of America.

Kevin T Oakes, CPA

Fredericksburg, VA
June 17, 2020

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED BALANCE SHEETS
DECEMBER 31, 2019 AND 2018

ASSETS

	2019	2018
Current Assets		
Cash	$ 1,784,213	$ 2,106,588
Accounts Receivable, net	2,085,414	2,202,640
Unbilled A/R	1,078,502	-
Construction in Process	119,910	454,688
Prepaid Expenses	1,042,522	819,492
	6,110,561	5,583,408
Property and Equipment		
Furniture and Equipment	308,752	285,302
Less: Accumulated Depreciation	(267,493)	(248,568)
	41,259	36,734
Intangible Asset		
Capitalized Software	412,749	412,749
Less: Accumulated Amortization	(412,749)	(412,749)
	-	-
Other Assets		
Deposits	14,537	14,537
Long Term Prepaid Expense	-	1,457
	14,537	15,994
Total Assets	$ 6,166,357	$ 5,636,136

See Independent Auditor's Report
See Accompanying Notes to Consolidated the Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED BALANCE SHEETS
DECEMBER 31, 2019 AND 2018

LIABILITIES AND STOCKHOLDERS' EQUITY

	2019	2018
Current Liabilities		
Accounts Payable	$ 2,256,582	$ 1,263,760
Accrued Expenses	361,594	406,864
Deferred Revenue	2,757,975	2,723,337
State Taxes Payable	33,463	33,463
	5,409,614	4,427,424
Total Liabilities	5,409,614	4,427,424
Stockholders' Equity		
Common stock, no par value, 20,000 shares authorized, issued and outstanding		
Additional paid-in capital	170,700	170,700
Equity Translation Adjustment	27,341	23,737
Retained Earnings	558,702	1,014,275
Total stockholders' equity	756,743	1,208,712
Total liabilities and stockholders' equity	$ 6,166,357	$ 5,636,136

See Independent Auditor's
See Accompanying Notes to Consolidated the Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED STATEMENTS OF OPERATIONS AND RETAINED EARNINGS
FOR THE YEARS ENDED DECEMBER 31, 2019 AND 2018

	2019	2018
Revenue		
Sales - Commercial and Government	$ 9,960,042	$ 9,170,600
Sales - Leased Equipment	174,311	178,211
Sales - Maintenance	7,596,516	7,508,715
Net Operating Revenue	17,730,869	16,857,526
Cost of Goods Sold	11,556,600	11,307,856
Gross Profit	6,174,269	5,549,670
Operating Expenses		
Depreciation and Amortization	18,924	24,254
Research and Development	929,507	1,020,629
General and Administrative	4,452,725	3,424,645
	5,401,156	4,469,528
Income from Operations	773,113	1,080,142
Other Income		
Interest Income	13,821	1,941
Interest Expense	(1,842)	-
Other Income	11,716	12,502
	23,695	14,443
Net Income Before Taxes	796,808	1,094,585
Provision for Taxes	7,840	23,340
Net Income	$ 788,968	$ 1,071,245
Retained Earnings		
Beginning of Year	1,014,275	711,812
Less: Distributions to Shareholders	(1,244,541)	(768,781)
End of Year	558,702	1,014,275

See Independent Auditor's Report
See Accompanying Notes to the Consolidated Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED STATEMENT OF CASH FLOWS
FOR THE YEARS ENDED DECEMBER 31, 2019 AND 2018

	2019	2018
Cash Flows from Operating Activities		
Net Income (Loss)	$ 788,968	$ 1,071,245
Reconciliation adjustments		
Depreciation and amortization	18,924	24,254
Bad Debt Expense	128,910	3,876
Changes in:		
Accounts receivable	(1,090,185)	(238,079)
Deposits and other	(221,573)	55,087
Construction in Process	334,778	(309,714)
Accounts Payable and Accrued Expenses	947,552	573,090
Deferred Revenue	34,638	(197,508)
Net cash provided by Operating Activities	942,012	982,251
Cash Flows from Investing Activities		
Net additions to property	(23,450)	(15,038)
Equity Translation Adjustment	3,604	(2,625)
Cash Flows from Financing Activities		
Shareholder Distributions	(1,244,541)	(768,781)
Net (decrease) increase in Cash and Cash Equivalents	(322,375)	195,807
Cash and Cash Equivalents, beginning of the year	2,106,588	1,910,781
Cash and Cash Equivalents, end of the year	$ 1,784,213	$ 2,106,588

Supplementary Cash Flow Information

Cash paid during the year for:		
Interest	1,842	-
State & Canada income taxes	7,840	23,340

See Independent Auditor's Report
See Accompanying Notes to the Consolidated Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
NOTES TO THE CONSOLIDATED FINANCIAL STATEMENTS
DECEMBER 31, 2019

1. Organization

Fairfax Imaging, Inc. (the Company) was incorporated on March 22, 1994, under the laws of the Commonwealth of Virginia, and is engaged as a developer of image scanning software and systems for commercial and governmental use. Fairfax Imaging (Vietnam) Co., Ltd., a 100% foreign-owned company was established by Fairfax Imaging, Inc. on December 21, 2006 with the investment certificate No. 411043000048 granted by the Ho Chi Minh City People's Committee. The operation period of Fairfax Imaging (Vietnam) Co., Ltd. is 20 years, starting from the date of the investment certificate.

2. Summary of Significant Accounting Policies

Basis of Accounting – The Company maintains its books under the accrual method of accounting in accordance with generally accepted accounting principles. The accrual basis of accounting provides that revenues and gains are recognized when earned and expenses and losses are recognized when incurred. Consolidated financial items are recorded at historical costs and often involve the utilization of estimates. Consequently, consolidated financial statement items do not necessarily represent current values.

Revenue and Cost Recognition – The Company enters into multiple deliverable arrangements which may include any combination of services to include sale of hardware to customization and implementation of software. A multiple deliverable arrangement is separated into more than one unit of accounting if all these criteria are met:

- The delivered item has value to the client on a stand-alone basis;
- There is no objective and reliable evidence of the fair value of the undelivered item; and
- Delivery is considered probable and is under the Company's control.

If these criteria are met for each element and there is no objective and reliable evidence of fair value for all units of accounting in an arrangement, the arrangement consideration is allocated to the separate units of accounting based on each unit's relative fair value.

The Company provides technical support to customers with maintenance contracts, on an as needed and if available basis. The Company recognizes customer support revenue, including support revenue that is bundled with product sales, ratably over the term of the contract period, which generally ranges from six months to one year. Revenues from services are recognized when the services are performed.

Revenue and Cost Recognition (continued)

Disputes arise in the normal course of the Company's business. The Company occasionally has disputes with customers for collection of funds because of events such as delays, changes in contract specifications, or questions of cost allowance or collection. Such disputes whether for claims or unapproved change orders, are recorded at the lesser of their estimated net realizable value or actual costs incurred when realization is probable and can be reliably estimated. Claims against the Company are recognized when loss is considered probable and the amount is reasonably determinable.

Depreciation – Depreciation is computed straight-line with computer equipment and software at 3 years while furniture and fixtures are at 7 years.

Research and Development – Research and Development costs are expensed as incurred. Costs incurred prior to establishment of technological feasibility are expensed as incurred and reflected as research and development expense in the accompanying consolidated statement of operations and retained earnings. For the year ended December 31, 2019, the Company did not capitalize any costs related to software development

Use of Estimates – The preparation of financial statements requires management to make estimates and assumptions that affect certain reported amounts and disclosures, including contract contingencies. Accordingly, actual results could differ from those estimates.

Cash and Cash Equivalents – The Company invests its cash solely in deposits with insured bank institutions. The total account balance periodically exceeds the Federal Deposit Insurance Corporation ("FDIC") insurance coverage. When this occurs there is a concentration of credit risk related to amounts on deposit in excess of FDIC insurance coverage. The risk is managed by maintaining all deposits in what management believes to be high quality institutions.

On November 9, 2010, the Federal Deposit Insurance Corporation (FDIC) issued a Final Rule implementing section 343 of the Dodd-Frank Wall Street Reform and Consumer Protection Act that provides for unlimited insurance coverage of non-interest bearing accounts. Beginning December 31, 2010 through December 31, 2012, all non-interest bearing accounts are fully insured, regardless of the balance of the account, at FDIC-insured institutions. Interest bearing accounts are insured up to a maximum deposit insurance amount of $250,000 per depositor per insured depository institutions. Beginning January 1, 2013, non-interest bearing accounts will no longer be insured separately from interest bearing accounts held at the same financial institution. All balances insured held at the same financial institution will be insured up to $250,000. As of December 31, 2019, cash balances exceeded FDIC limitations by $1,109,085. The Company does not consider this to be a material risk.

Construction in Process – Construction in process consists of supplies delivered to customer locations and undergoing on-site installation.

Accounts Receivable – Accounts receivable is recorded at the amount the Company expects to collect on balances outstanding at year-end. Management closely monitors outstanding balances and write-offs throughout the year balances that have been deemed uncollectible. Bad debts in 2019 and 2018, respectively were $128,910 and $3,876. As of December 31, 2019, all accounts receivable were deemed collectible.

Advertising – Advertising costs are expensed as they are incurred. Advertising costs in 2019 and 2018 respectively were $948 and $0.

Income Taxes – The Company, with the consent of its shareholders, has elected to be treated as an S Corporation under the provisions of the Internal Revenue Code. In lieu of federal corporation income taxes, the shareholders of an S Corporation are taxed on their proportionate share of the Company's taxable income or losses for federal tax reporting purposes. The Company is subject to state taxes in thirty-two states as the Company operates in those states and those states assess tax on S Corporations. The Company is also subject to tax in Canada and Vietnam.

Effective January 1, 2009, the Company implemented the accounting guidance for uncertainty in income taxes using provisions of Financial Accounting Standards Board (FASB) ASC 740, *Income Taxes*. Using that guidance, tax positions initially need to be recognized in the consolidated financial statements when it is more likely than not the position will be sustained upon examination by the tax authorities.

As of December 31, 2019, the Company had no uncertain tax positions that qualify for either recognition or disclosure in the consolidated financial statements.

With few exceptions, the Company is no longer subject to US federal and state income tax examinations by tax authorities for years prior to 2017.

3. Investments

In 2007, Fairfax Imaging, Inc. established Fairfax Imaging (Vietnam) Co., Ltd., a 100% foreign owned Company. Fairfax Imaging (Vietnam) Co., Ltd. incurred a net loss in the amount of $337,659 for the year ended December 31, 2019 and a net loss in the amount of $316,225 for the year ended December 31, 2018. This investment has been accounted for under the consolidation method. Under the consolidation method, the financial statements of the investee are combined with those of the investor and intercompany amounts are eliminated. For tax purposes, Fairfax Imaging (Vietnam) Co., Ltd. is taxed as a separate entity under Vietnam tax laws.

4. Line of Credit

The Revolving Loan and Security Agreement with Valley National Bank, formerly USAmeribank, for short-term borrowings of $2,750,000 under two line of credit agreements, one for $2,000,000 and one for $750,000, which bear interest at the U.S. Prime Rate had no balance due as of December 31, 2019.

5. Commitments and Contingencies

In order to provide certain parts and equipment to fulfill applicable sales orders, the Company has entered into multiple contracts with suppliers for the purchase and manufacture of equipment. The Company is exposed to contingent liabilities regarding outstanding purchase orders with the suppliers. The amounts and limitations of any loss attributable to the Company would be conditioned upon the contract specifications governing the related purchase order.

Management estimates the maximum loss at December 31, 2019, assuming non-performance by the Company on all outstanding contracts, to be less than $50,000.

6. Economic Dependency

For the year ended December 31, 2019, management estimates that 25% of gross sales were received from commercial customers and 75% from the Canadian, Vietnamese, U.S. and State governments. No single customer accounted for more than 15% of sales.

7. Leases

The Company leases certain facilities and equipment under operating leases expiring at various dates. Rent expense for the office facilities under operating leases was $221,548 for 2019 and $226,915 for 2018. Future minimum rental obligations are as follows:

For the year ending December 31, 2020	$ 162,431
2021	167,494
2022	172,557
2023	72,778
2024	0
	$ 575,260

8. Employee Benefit Plan

The company maintains a 401(k) Profit Sharing Plan. The plan covers all employees of the Company. The Company makes a 4% mandatory safe harbor matching contribution to the plan annually. Total contribution expense was $155,919 for the year ended December 31, 2019 and $146,715 for the year ended December 31, 2018.

9. Income Taxes

As a result of its S election, the Company is not subject to federal income tax but is subject to income tax in certain states, Canada, and Vietnam. The Company has elected to file Composite State Income Tax Returns where applicable. Payments due with the composite returns are treated as distributions to shareholders. The provision for income taxes in 2019 was $7,840 and in 2018 was $23,340.

10. Related Party Transactions

Software Consultants of Tampa Bay, Inc was formed on October 29, 2018. The corporation is 100% owned by the shareholder of Fairfax Imaging, Inc. During 2019, invoices totaling $55,000 were issued to Fairfax Imaging, Inc. As of December 31, 2019, these amounts were payable to Software Consultants of Tampa Bay, Inc.

11. Subsequent Events

In preparing the financial statements, the Company has evaluated events and transactions for potential recognition or disclosure through June 17, 2020, the date that the financial statements were available to be issued.

.

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED SCHEDULE OF GENERAL AND ADMINISTRATIVE EXPENSES
FOR THE YEARS ENDED DECEMBER 31, 2019 AND 2018

	2019	2018
Salaries	$ 866,151	$ 765,072
Repairs	2,177	-
Bad Debt	128,910	3,876
Rent	221,548	226,915
Property, Sales, and Other Taxes	449,240	409,924
Advertising	948	-
Employee Benefits	218,029	161,039
Automobile	8,279	3,500
Bank Fees	30,622	17,860
Consulting	568,984	360,672
Contributions	1,236	-
Dues	84,538	45,072
Employee Training	13,816	2,490
Insurance	769,438	774,942
Licenses	15,993	1,109
Maintenance	2,985	2,469
Meals and Entertainment	43,818	15,392
Miscellaneous	3,515	3,618
Computer and Office Supplies	77,164	27,738
Payroll Processing	13,729	14,885
Penalties	45	-
Postage	68,607	8,149
Printing	4,936	212
Professional Fees	253,469	258,805
Recruitment	4,420	11,816
Relocation	11,494	10,775
Seminars	-	1,494
Telephone	87,275	100,996
Temporary Assistance	-	3,948
Trade Show	48,739	6,008
Travel	452,620	185,869
Total	$ 4,452,725	$ 3,424,645

FAIRFAX IMAGING, INC. AND SUBSIDIARY

FINANCIAL STATEMENTS

WITH SUPPLEMENTARY INFORMATION

AND INDEPENDENT AUDITOR'S REPORT

DECEMBER 31, 2020 AND 2019

FAIRFAX IMAGING, INC AND SUBSIDIARY
CONSOLIDATED FINANCIAL STATEMENTS
DECEMBER 31, 2020 AND 2019

Contents

	Page
Independent Auditor's Report	1
Consolidated Balance Sheets	2-3
Consolidated Statement of Operations and Retained Earnings	4
Consolidated Statement of Cash Flows	5
Notes to the Consolidated Financial Statements	6-10
Consolidated Schedules of General and Administrative Expenses	11

OAKES, P.C.

3330 BOURBON STREET, SUITE 102
FREDERICKSBURG, VIRGINIA 22408
PHONE (540) 371-1300
FAX (540) 373-6172

INDEPENDENT AUDITOR'S REPORT

Board of Directors
Fairfax Imaging, Inc.
Tampa, Florida

We have audited the accompanying consolidated balance sheets of Fairfax Imaging, Inc. (an S Corporation) and subsidiary as of December 31, 2020 and 2019, and the related statements of operations and retained earnings and cash flows for the years then ended.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Subsidiary

We did not audit the financial statements for the years ended December 31, 2020 and 2019 of Fairfax Imaging (Vietnam) Co., Ltd, a consolidated subsidiary, whose statements reflect total assets and expenses constituting less than 1% of the related consolidated totals. The results of our audit expressed herein, insofar as it relates to the above is based solely upon the report of other auditors and accountants.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Fairfax Imaging, Inc. and subsidiary as of December 31, 2020 and 2019, and the results of its operations and its cash flows for the years then ended in conformity with generally accepted accounting principles in the United States of America.

Kevin T Oakes, CPA

Fredericksburg, VA
July 30, 2021

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED BALANCE SHEETS
DECEMBER 31, 2020 AND 2019

ASSETS

	2020	2019
Current Assets		
Cash	$ 2,136,222	$ 1,784,213
Accounts Receivable, net	2,519,415	2,085,414
Unbilled A/R	14,988	1,078,502
Construction in Process	535,907	119,910
Prepaid Expenses	954,515	1,042,522
Supplies	309,534	-
	6,470,581	6,110,561
Property and Equipment		
Furniture and Equipment	332,096	308,752
Less: Accumulated Depreciation	(286,315)	(267,493)
	45,781	41,259
Intagible Asset		
Capitalized Sofware	412,749	412,749
Less: Accumulated Depreciation	(412,749)	(412,749)
	-	-
Other Assets		
Deposits	14,957	14,537
Long Term Prepaid Expense	322	-
	15,279	14,537
Total Assets	$ 6,531,641	$ 6,166,357

See Independent Auditor's Report
See Accompanying Notes to Consolidated the Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED BALANCE SHEETS
DECEMBER 31, 2020 AND 2019

LIABILITIES AND STOCKHOLDERS' EQUITY

	2020	2019
Current Liabilities		
Accounts Payable	$ 1,349,325	$ 2,256,582
Accrued Expenses	596,945	361,594
Deferred Revenue	2,624,177	2,757,975
SBA PPP Loan	1,148,255	-
State Taxes Payable	33,463	33,463
	5,752,165	5,409,614
Total Liabilities	5,752,165	5,409,614
Stockholders' Equity		
Common stock, no par value, 1,000 shares authorized, issued and outstanding		
Additional paid-in capital	170,700	170,700
Equity Translation Adjustment	27,427	27,341
Retained Earnings	581,349	558,702
Total stockholders' equity	779,476	756,743
Total liabilities and stockholders' equity	$ 6,531,641	$ 6,166,357

See Independent Auditor's
See Accompanying Notes to Consolidated the Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED STATEMENTS OF OPERATIONS AND RETAINED EARNINGS
FOR THE YEARS ENDED DECEMBER 31, 2020 AND 2019

	2020	2019
Revenue		
Sales - Commercial and Government	$ 10,656,753	$ 9,960,042
Sales - Leased Equipment	154,078	174,311
Sales - Maintenance	7,824,754	7,596,516
Net Operating Revenue	18,635,585	17,730,869
Cost of Goods Sold	11,557,250	11,556,600
Gross Profit	7,078,335	6,174,269
Operating Expenses		
Depreciation and Amortization	18,822	18,924
Research and Development	715,588	929,507
General and Administrative	4,817,616	4,452,725
	5,552,026	5,401,156
Income from Operations	1,526,309	773,113
Other Income		
Interest Income	6,850	13,821
Interest Expense	-	(1,842)
Other Income	20,069	11,716
	26,919	23,695
Net Income Before Taxes	1,553,228	796,808
Provision for Taxes	16,154	7,840
Net Income	$ 1,537,074	$ 788,968
Retained Earnings		
Beginning of Year	558,702	1,014,275
Add: Prior Period Adjustments	162,238	-
Less: Distributions to Shareholders	(1,676,665)	(1,244,541)
End of Year	581,349	558,702

See Independent Auditor's Report
See Accompanying Notes to the Consolidated Financial Statements

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED STATEMENT OF CASH FLOWS
FOR THE YEARS ENDED DECEMBER 31, 2020 AND 2019

	2020	2019
Cash Flows from Operating Activities		
Net Income (Loss)	$ 1,537,074	$ 788,968
Reconciliation adjustments		
Depreciation and amortization	18,822	18,924
Bad Debt Expense	-	128,910
Changes in:		
Accounts receivable	629,513	(1,090,185)
Supplies	(309,534)	-
Deposits and other	87,265	(221,573)
Construction in Process	(415,997)	334,778
Accounts Payable and Accrued Expenses	(671,906)	947,552
Deferred Revenue	(133,798)	34,638
Net cash provided by Operating Activities	741,439	942,012
Cash Flows from Investing Activities		
Net additions to property	(23,344)	(23,450)
Equity Translation Adjustment	86	3,604
Cash Flows from Financing Activities		
SBA PPP Loan	1,148,255	-
Prior Period Adjustment	162,238	-
Shareholder Distributions	(1,676,665)	(1,244,541)
Net (decrease) increase in Cash and Cash Equivalents	352,009	(322,375)
Cash and Cash Equivalents, beginning of the year	1,784,213	2,106,588
Cash and Cash Equivalents, end of the year	$ 2,136,222	$ 1,784,213

Supplementary Cash Flow Information

Cash paid during the year for:		
Interest	6,850	1,842
State & Canada income taxes	16,154	7,840

See Independent Auditor's Report
See Accompanying Notes to the Consolidated Financial Statements

1. Organization

Fairfax Imaging, Inc. (the Company) was incorporated on March 22, 1994, under the laws of the Commonwealth of Virginia, and is engaged as a developer of image scanning software and systems for commercial and governmental use. Fairfax Imaging (Vietnam) Co., Ltd., a 100% foreign-owned company was established by Fairfax Imaging, Inc. on December 21, 2006 with the investment certificate No. 411043000048 granted by the Ho Chi Minh City People's Committee. The operation period of Fairfax Imaging (Vietnam) Co., Ltd. is 20 years, starting from the date of the investment certificate.

2. Summary of Significant Accounting Policies

Basis of Accounting – The Company maintains its books under the accrual method of accounting in accordance with generally accepted accounting principles. The accrual basis of accounting provides that revenues and gains are recognized when earned and expenses and losses are recognized when incurred. Consolidated financial items are recorded at historical costs and often involve the utilization of estimates. Consequently, consolidated financial statement items do not necessarily represent current values.

Revenue and Cost Recognition – The Company enters into multiple deliverable arrangements which may include any combination of services to include sale of hardware to customization and implementation of software. A multiple deliverable arrangement is separated into more than one unit of accounting if all these criteria are met:

- The delivered item has value to the client on a stand-alone basis;
- There is no objective and reliable evidence of the fair value of the undelivered item; and
- Delivery is considered probable and is under the Company's control.

If these criteria are met for each element and there is no objective and reliable evidence of fair value for all units of accounting in an arrangement, the arrangement consideration is allocated to the separate units of accounting based on each unit's relative fair value.

The Company provides technical support to customers with maintenance contracts, on an as needed and if available basis. The Company recognizes customer support revenue, including support revenue that is bundled with product sales, ratably over the term of the contract period, which generally ranges from six months to one year. Revenues from services are recognized when the services are performed.

Revenue and Cost Recognition (continued)

Disputes arise in the normal course of the Company's business. The Company occasionally has disputes with customers for collection of funds because of events such as delays, changes in contract specifications, or questions of cost allowance or collection. Such disputes whether for claims or unapproved change orders, are recorded at the lesser of their estimated net realizable value or actual costs incurred when realization is probable and can be reliably estimated. Claims against the Company are recognized when loss is considered probable and the amount is reasonably determinable.

Depreciation – Depreciation is computed straight-line with computer equipment and software at 3 years while furniture and fixtures are at 7 years.

Research and Development – Research and Development costs are expensed as incurred. Costs incurred prior to establishment of technological feasibility are expensed as incurred and reflected as research and development expense in the accompanying consolidated statement of operations and retained earnings. For the year ended December 31, 2020, the Company did not capitalize any costs related to software development

Use of Estimates – The preparation of financial statements requires management to make estimates and assumptions that affect certain reported amounts and disclosures, including contract contingencies. Accordingly, actual results could differ from those estimates.

Cash and Cash Equivalents – The Company invests its cash solely in deposits with insured bank institutions. The total account balance periodically exceeds the Federal Deposit Insurance Corporation ("FDIC") insurance coverage. When this occurs there is a concentration of credit risk related to amounts on deposit in excess of FDIC insurance coverage. The risk is managed by maintaining all deposits in what management believes to be high quality institutions.

On November 9, 2010, the Federal Deposit Insurance Corporation (FDIC) issued a Final Rule implementing section 343 of the Dodd-Frank Wall Street Reform and Consumer Protection Act that provides for unlimited insurance coverage of non-interest bearing accounts. Beginning December 31, 2010 through December 31, 2012, all non-interest bearing accounts are fully insured, regardless of the balance of the account, at FDIC-insured institutions. Interest bearing accounts are insured up to a maximum deposit insurance amount of $250,000 per depositor per insured depository institutions. Beginning January 1, 2013, non-interest bearing accounts will no longer be insured separately from interest bearing accounts held at the same financial institution. All balances insured held at the same financial institution will be insured up to $250,000. As of December 31, 2020, cash balances exceeded FDIC limitations by $662,774. The Company does not consider this to be a material risk.

Construction in Process – Construction in process consists of supplies delivered to customer locations and undergoing on-site installation.

Accounts Receivable – Accounts receivable is recorded at the amount the Company expects to collect on balances outstanding at year-end. Management closely monitors outstanding balances and write-offs throughout the year balances that have been deemed uncollectible. Bad debts in 2020 and 2019, respectively were $0 and $128,910. As of December 31, 2020, all accounts receivable were deemed collectible.

Advertising – Advertising costs are expensed as they are incurred. Advertising costs in 2020 and 2019 respectively were $57 and $948.

Income Taxes – The Company, with the consent of its shareholders, has elected to be treated as an S Corporation under the provisions of the Internal Revenue Code. In lieu of federal corporation income taxes, the shareholders of an S Corporation are taxed on their proportionate share of the Company's taxable income or losses for federal tax reporting purposes. The Company is subject to state taxes in thirty-two states as the Company operates in those states and those states assess tax on S Corporations. The Company is also subject to tax in Canada and Vietnam.

Effective January 1, 2009, the Company implemented the accounting guidance for uncertainty in income taxes using provisions of Financial Accounting Standards Board (FASB) ASC 740, *Income Taxes*. Using that guidance, tax positions initially need to be recognized in the consolidated financial statements when it is more likely than not the position will be sustained upon examination by the tax authorities.

As of December 31, 2020, the Company had no uncertain tax positions that qualify for either recognition or disclosure in the consolidated financial statements.

With few exceptions, the Company is no longer subject to US federal and state income tax examinations by tax authorities for years prior to 2018.

3. Investments

In 2007, Fairfax Imaging, Inc. established Fairfax Imaging (Vietnam) Co., Ltd., a 100% foreign owned Company. Fairfax Imaging (Vietnam) Co., Ltd. incurred a net loss in the amount of $354,877 for the year ended December 31, 2020 and a net loss in the amount of $337,654 for the year ended December 31, 2019. This investment has been accounted for under the consolidation method. Under the consolidation method, the financial statements of the investee are combined with those of the investor and intercompany amounts are eliminated. For tax purposes, Fairfax Imaging (Vietnam) Co., Ltd. is taxed as a separate entity under Vietnam tax laws.

4. Line of Credit

The Revolving Loan and Security Agreement with Valley National Bank, formerly USAmeribank, for short-term borrowings of $2,750,000 under two line of credit agreements, one for $2,000,000 and one for $750,000, which bear interest at the U.S. Prime Rate had no balance due as of December 31, 2020.

5. Commitments and Contingencies

In order to provide certain parts and equipment to fulfill applicable sales orders, the Company has entered into multiple contracts with suppliers for the purchase and manufacture of equipment. The Company is exposed to contingent liabilities regarding outstanding purchase orders with the suppliers. The amounts and limitations of any loss attributable to the Company would be conditioned upon the contract specifications governing the related purchase order.

Management estimates the maximum loss at December 31, 2020, assuming non-performance by the Company on all outstanding contracts, to be less than $50,000.

6. Economic Dependency

For the year ended December 31, 2020, management estimates that 25% of gross sales were received from commercial customers and 75% from the Canadian, Vietnamese, U.S. and State governments. No single customer accounted for more than 15% of sales.

7. Leases

The Company leases certain facilities and equipment under operating leases expiring at various dates. Rent expense for the office facilities under operating leases was $232,089 for 2020 and $221,548 for 2019. Future minimum rental obligations are as follows:

For the year ending December 31, 2021	$ 207,693
2022	210,417
2023	72,778
2024	0
2025	0
	$ 490,888

8. Employee Benefit Plan

The company maintains a 401(k) Profit Sharing Plan. The plan covers all employees of the Company. The Company makes a 4% mandatory safe harbor matching contribution to the plan annually. Total contribution expense was $160,710 for the year ended December 31, 2020 and $155,919 for the year ended December 31, 2019.

9. Income Taxes

As a result of its S election, the Company is not subject to federal income tax but is subject to income tax in certain states, Canada, and Vietnam. The Company has elected to file Composite State Income Tax Returns where applicable. Payments due with the composite returns are treated as distributions to shareholders. The provision for income taxes in 2020 was $16,114 and in 2019 was $7,840.

10. Related Party Transactions

Software Consultants of Tampa Bay, Inc was formed on October 29, 2018. The corporation is 100% owned by the shareholder of Fairfax Imaging, Inc. During 2020, invoices totaling $69,480 were issued to Fairfax Imaging, Inc. As of December 31, 2020, no amounts were payable to Software Consultants of Tampa Bay, Inc.

11. Prior Period Adjustment

During the 2019, the Company transitioned to a new accounting software application. During the transitions, there were duplicate entries of accounts receivable in the amount of $15,190, and accounts payable and accrued expenses in the amount of $177,428. The net effect of the duplicate entries $162,238 has been reported as an increase to retained earnings on the Consolidated Statements of Operations and Retained Earnings.

12. Subsequent Events

In preparing the financial statements, the Company has evaluated events and transactions for potential recognition or disclosure through July 30, 2021, the date that the financial statements were available to be issued.

FAIRFAX IMAGING, INC. AND SUBSIDIARY
CONSOLIDATED SCHEDULE OF GENERAL AND ADMINISTRATIVE EXPENSES
FOR THE YEARS ENDED DECEMBER 31, 2020 AND 2019

	2020	2019
Salaries	$ 1,824,868	$ 866,151
Repairs	3,301	2,177
Bad Debt	-	128,910
Rent	232,089	221,548
Property, Sales, and Other Taxes	457,573	449,240
Advertising	57	948
Employee Benefits	162,344	218,029
Automobile	8,400	8,279
Bank Fees	20,496	30,622
Consulting	352,573	568,984
Contributions	-	1,236
Compliance/Security	225,381	-
Dues	99,742	84,538
Employee Training	555	13,816
Insurance	675,263	769,438
Licenses	53,300	15,993
Maintenance	7,835	2,985
Meals and Entertainment	25,691	43,818
Miscellaneous	4,348	3,515
Computer and Office Supplies	87,099	77,164
Payroll Processing	11,823	13,729
Penalties	153	45
Postage	40,296	68,607
Printing	250	4,936
Professional Fees	274,701	253,469
Recruitment	26,110	4,420
Relocation	22	11,494
Telephone	82,801	87,275
Trade Show and Marketing Materials	27,636	48,739
Travel	112,909	452,620
Total	$ 4,817,616	$ 4,452,725

ATTACHMENT D – REFERENCES

Proposers must provide a minimum of three (3) references from three local government or state governmental entities for whom equal or larger scope of services are either currently being provided or have been provided in recent past (not more than one year). Contact person(s), addresses and telephone numbers for each reference shall be included.

Fairfax Software Response:

Fairfax Software has been providing payment services, forms, and remittance processing systems for twenty-seven (27) years. We started performing financial transaction processing before payment portals even existed. However, we realized the principles of payment acceptance are the same whether done by mail, over the counter, or via payment portals. Our same common system accepts all three forms of payments making it the most universal system of its kind in the world made by the same reliable and responsible vendor. With the advent of the cloud technologies and the payment portals we started applying the technologies and the know-how that we acquired over two decades to the payment portal solution, hence our *Quick* Payments signature product. The initial release of the innovative *Quick* Payments product was in 2016. We have over 100 customers processing billions of dollars per day using our software.

Reference 1:

REFERENCE		
1.	Organization Name	New Zealand Ministry of Business, Innovation and Employment (MBIE). 15 Stout St., Wellington, New Zealand
2.	Contact Person	Simon Ferguson, Business Systems Manager, Service Transformation
3.	Telephone	Phone: +64 4 978 3692
4.	Email	Mr. Ferguson can be easily reached via email at simon.ferguson@mbie.govt.nz
5.	Length and Dates of Services	June 2016 to Present
6.	Description of Services	New Zealand saw the need to offer citizens more electronic payment options while delivering a consistent payment experience. Fairfax Software implemented its Quick Payments System to provide a shared payment service across all business units. • Integrated Quick Payments System • 5,854,000 transactions processed to date • Handles cash, credit card, and direct debit (New Zealand equivalent to ACH) transactions for t over 20 New Zealand government agencies. Each agency has their own unique business rules and processing requirements set up in point-and-click system templates.

		• Functionality includes automatic statement generation, electronic delivery, and notification to citizens for bills with an amount due. • Quick Payments offers citizens the same payment system across all agencies.

Reference 2:

REFERENCE		
1.	Organization Name	Colorado Bureau of Investigation 700 Kipling Street, Denver CO 80215
4.	Contact Person	Jessica Anderson, Accountant Financial Services
3.	Telephone	(303) 239-5728
4.	Email	Ms. Anderson can easily be reached via email at Jessica.anderson@state.co.us
5.	Length and Dates of Services	June 2017 to Present
6.	Description of Services	The CBI supports three different business units within the agency with electronic payments functionality including: • The Identification Unit for collecting fees and annual dues from state and local Colorado agencies that use the CBI's Background Search services. • The Toxicology unit for collecting fees for laboratory services provided to local Colorado agencies and the general public • The InstaCheck unit for collecting fees for performing criminal background checks for local Colorado agencies and companies that require pre-employment testing. CBI *Quick* Payments functionality includes: • Web-based and walk-up payments accepted • Approval workflow for auto pay setup on behalf of a state agency • *Quick* Payments is integrated with each business unit. Strict confidentiality requires that each business unit be autonomous, and data cannot be shared between business units. An administrator for a business unit cannot access data in another business unit. • Handles cash, check, and credit card

		• A monthly receipt of invoice files is received from the host system, invoices are created and distributed electronically for payment. • Full service on-line payment portal for employers and government agencies in Colorado.

Reference 3:

REFERENCE		
1.	Organization Name	Hawaii County Department of Finance Hilo, Hawaii
2.	Contact Person	Chris Nakano, Treasury Division Manager
3.	Telephone	(808) 933-6240
4.	Email	Mr. Nakano can easily be reached via email at Chris.Nakano@hawaiicounty.com
5.	Length and Dates of Services	January 2022 to Present
6.	Description of Services	Fairfax Software implemented its online Quick Payments module to provide a full featured payment system that processes electronic online payments and provides the ability to process refunds, and credits. The solution also creates and manages invoices, recurring statements, automatic payments, payment plans, and provides back-end accounting system integration. For over-the-counter payments (OTC), Fairfax Software implemented its Quick Modules Cashiering that manages the OTC payment collection process and activities from multiple collection sources and consolidates these transactions with updating to the counties accounting and finance systems.

360 ADVANCED

January 25, 2022

Nadine Chahal
Fairfax Imaging, Inc.
2005 Pan Am Circle, STE 110
Tampa, FL 33607

To the Management of Fairfax Imaging, Inc.:

This letter is to confirm that 360 Advanced, Inc., an authorized Payment Card Industry Qualified Security Assessor for the North America region, completed Payment Card Industry Report on Compliance Procedures for the Quick Modules system provided by Fairfax Imaging, Inc. at the Tampa, Florida facility. Procedures were conducted via virtual walkthroughs, demonstrations, and interviews due to the COVID-19 pandemic. All relevant requirements were deemed to be "In Place". Results of the December 8, 2021 assessment were agreed and signed to in the Attestation of Compliance (AOC) on January 25, 2022.

Please contact Chris Gudzak at cgudzak@360advanced.com should you have any questions.

Best regards,

360 Advanced

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	Fairfax Imaging, Inc.		DBA (doing business as):	Fairfax Software	
Contact Name:	Steve Chahal		Title:	Co-founder / President	
Telephone:	(877) 627-8325		E-mail:	schahal@ffximg.com	
Business Address:	2005 Pan Am Circle, Ste		City:	Tampa	
State/Province:	Florida	Country:	USA	Zip:	33607
URL:	www.fairfaximaging.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	360 Advanced, Inc.				
Lead QSA Contact Name:	Phillip Hagan		Title:	Technical Services Manager	
Telephone:	1-866-418-1708		E-mail:	phagan@360advanced.com	
Business Address:	200 Central Ave., Suite 2105		City:	St. Petersburg	
State/Province:	FL	Country:	United States	Zip:	33701
URL:	http://www.360advanced.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Quick Modules and Quick Cashier	
Type of service(s) assessed:		
Hosting Provider: ☒ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☒ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☒ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:	Quick Payments and Quick Tags	
Type of service(s) not assessed:		
Hosting Provider: ☒ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☒ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☒ Merchant Services	☒ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:	Quick Tags and Quick Modules have separate PCI-DSS CDE's and undergo their own PCI-DSS assessments.	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	**Transmission of potential CHD** The Fairfax Quick Modules flow of cardholder data begins with the receipt of payment authorization forms as paper material. This form is then scanned into a designated Fairfax workstation using an assigned Quick Modules scanner device for temporary storage. The image of the form is directly uploaded to the Quick Modules platform hosted solely within Amazon Web Services cloud environment. This image file is securely transferred using TLS v1.2. Quick Cashier is the front-end web application on the client-owned cashier workstations. QuickCashier interfaces with client middleware which in turn communicates with the Point-of-Sale device APIs to facilitate the credit card swipe. QuickCashier also allows for manual entry of the credit card by a cashier. The client middleware performs the CC encryption / decryption process by receiving the encrypted credit card data from the POS device and passing it to the description service via HTTPS and received back the decrypted CC data.

	The decrypted CC data is sent to the client-selected payment gateway for tokenization via HTTPS. Next the CC token and line-item information is sent to the payment gateway via HTTPs to assess fees. After the customer accepts the charges the CC token is submitted via HTTPS to the payment gateway for processing. Once the payment is processed the payment summary is sent to QuickCashier to complete the cashiering transaction. Communication between the QuickCashier front end and any client middleware is completes utilizing a web service local call via Java-script. **Processing of CHD** The flow of information scanned from a paper authorization form is as follows: ➢ The Quick Modules platform receives the image potentially containing CHD and stores it in an encrypted EBS volume ➢ The image is run through the Quick Modules' Optical Character Recognition (OCR) engine where potential CHD is extracted and stored within a database residing in an encrypted EBS volume ➢ Reporting output of potential CHD is determined by the client and then exchanged using a secure method via either SFTP or HTTPS ➢ Clients will then process payments though their own payment processors. This is independent from Fairfax's own payment services such as Quick Payments and is deemed out of scope of this assessment. Processing of CC information for Quick Cashier is handled via the client middleware transmissions utilizing HTTPS to and from a third-party (Fidelity Information Services (FIS)) payment gateway. **Storage of potential Cardholder Data** Storage of Quick Modules cardholder data is potentially in the form of both hard copy material and electronic media. Hard copy material potentially containing CHD printed or written on payment authorization forms are stored securely within a data processing room located within the Fairfax office in Tampa, FL while electronic copies and extracted CHD are stored encrypted within the cloud-hosted environment at AWS. Storage of QuickCashier data is the tokenized CC information and any related cashiering transaction details returned by the FIS payment gateway.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Fairfax Software provides workflow services via document imaging and automated data capture solutions to facilitate secure customer payments for their clients. Quick Cashier processes in-person credit card payments. Quick Modules converts physical forms to a digital copy to extract relevant payment fields using recognition technology.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Office	1	Tampa, FL
Amazon Web Services	Cloud	US East (N. Virginia)

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).*	Fairfax potentially receives, stores, and transmits CHD as a requirement of its services being provided via document imaging and automated data capture solutions. The origination of Quick Modules cardholder data comes in the form of paper authorization forms which are received at the Fairfax corporate office in Tampa and stored within a

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	secure data processing room. The form is then scanned, and the image temporarily stored on a secure workstation that transmits the image to the Quick Modules environment hosted in AWS. The image is stored within a SQL database to be processed using an OCR engine to extract the CHD from pre-defined fields. This information is also stored within the database and used to create an output file to be sent to the client using either SFTP or HTTPS. Quick Cashier is the front-end web application on the client-owned cashier workstations. QuickCashier interfaces with client middleware which in turn communicates with the Point-of-Sale device APIs to facilitate the credit card swipe. QuickCashier also allows for manual entry of the credit card by a cashier. The client middleware performs the CC encryption / decryption process by receiving the encrypted credit card data from the POS device and passing it to the description service via HTTPS and receiving back the decrypted CC data. The decrypted CC data is sent to the client-selected payment gateway for tokenization via HTTPS. Next the CC token and line-item information is sent to the payment gateway via HTTPs to assess fees. After the customer accepts the charges the CC token is submitted via HTTPS to the payment gateway for processing. Once the payment is processed the payment summary is sent to QuickCashier to complete the cashiering transaction. Communication between the QuickCashier front end and any client middleware is completed utilizing a web service local call via Java-script. Fairfax does not perform payment processing throughout this workflow.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☐ Yes ☒ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No
If Yes:	

Name of service provider:	**Description of services provided:**
Amazon Web Services	Data Center and Hosting Services
FIS	Payment Service Provider

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website*.

Name of Service Assessed:	Quick Modules

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	1.3.6 was not applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.
Requirement 2:	☐	☒	☐	2.1.1 was not applicable. Fairfax's CDE resided solely within their hosted infrastructure provided by AWS, a Level 1 PCI DSS-validated service provider, who prohibit wireless connections within the hosted infrastructure. 2.2.3 was not applicable. Fairfax validated that insecure services, daemons, or protocols are not enabled. 2.6 was not applicable. 360 Advanced verified that Fairfax is not serving as a shared hosting provider to their customers
Requirement 3:	☐	☒	☐	3.2 was not applicable. Fairfax is neither an issuer nor does not offer issuing support services. In addition, Fairfax does not store sensitive authentication data such as card validation codes / values, full track data, PINs, and PIN blocks.

				3.6 was not applicable. Fairfax does not share encryption keys with its customers or entities outside of the organization. 3.6.6 was not applicable. Fairfax does not perform manual clear-text cryptographic key-management operations.
Requirement 4:	☐	☒	☐	4.1.1 was not applicable. Fairfax's CDE resided solely within their hosted infrastructure provided by AWS, a PCI-compliant Level-1 Service Provider, who prohibited wireless connections within the hosted infrastructure.
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5 was not applicable. Fairfax did not have vendors who accessed system components within the CDE. 8.5.1 was not applicable. Fairfax did not require or maintain remote access to customer sites or systems. 8.7 was not applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.
Requirement 9:	☐	☒	☐	9.9 – 9.9.3 were not applicable. Fairfax does not support or manage point of sale devices that capture payment card data via direct physical interaction.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.3.4 and 11.3.4.1 were not applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.
Requirement 12:	☐	☒	☐	12.3.9 was not applicable. Fairfax did not provide vendors access to systems within the CDE.

				12.3.10 was not applicable. Fairfax implemented tokenization of cardholder data and did not store cardholder data within the environment.
Appendix A1:	☐	☐	☒	All of Appendix A1 was not applicable. Fairfax offers no services to PCI customers that would classify them as a shared hosting provider.
Appendix A2:	☐	☐	☒	All of Appendix A2 was not applicable. Fairfax does not support or manage point of sale devices that capture payment card data via direct physical interaction.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	December 8, 2021	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated December 8, 2021**.**

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Fairfax Imaging, Inc.* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Aperia*

Part 3b. Service Provider Attestation

DocuSigned by:
4067964DE278478...

Signature of Service Provider Executive Officer ↑	*Date:* January 25, 2022
Service Provider Executive Officer Name: Steve Chahal	*Title:* Co-Founder / President

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	360 Advanced provided PCI DSS assessment and system compliance services.

DocuSigned by:
601F853A03E7450...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* January 25, 2022
Duly Authorized Officer Name: Christopher Gudzak	*QSA Company:* 360 Advanced, Inc.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	

PCI Security Standards Council

360 ADVANCED

Payment Card Industry (PCI)

Data Security Standard

Report on Compliance for Fairfax Imaging, Inc.

PCI DSS v3.2.1 Template for Report on Compliance

Revision 1.0

June 2018

Document Changes

Date	Version	Description
February 2014	PCI DSS 3.0, Revision1.0	To introduce the template for submitting Reports on Compliance. *This document is intended for use with version 3.0 of the PCI Data Security Standard.*
July 2014	PCI DSS 3.0, Revision 1.1	Errata - Minor edits made to address typos and general errors, slight addition of content
April 2015	PCI DSS 3.1, Revision1.0	Revision to align with changes from PCI DSS 3.0 to PCI DSS 3.1 (see *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1* for details of those changes). Also includes minor edits made for clarification and/or format.
April 2016	PCI DSS 3.2, Revision 1.0	Revision to align with changes from PCI DSS 3.1 to PCI DSS 3.2 (see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2* for details of those changes). Also includes minor corrections and edits made for clarification and/or format.
June 2018	PCI DSS 3.2.1 Revision 1.0	Revision to align with changes from PCI DSS 3.2 to PCI DSS 3.2.1 (see *PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1* for details of changes). Also includes minor corrections and edits made for clarification and/or format.

Table of Contents

Document Changes ..... **ii**

Introduction to the ROC Template **1**

ROC Template for PCI Data Security Standard v3.2.1 ..... **8**

1. Contact Information and Report Date **8**

1.1 Contact information *8*

1.2 Date and timeframe of assessment *9*

1.3 PCI DSS version *10*

1.4 Additional services provided by QSA company *10*

1.5 Summary of Findings *11*

2. Summary Overview **12**

2.1 Description of the entity's payment card business *12*

2.2 High-level network diagram(s) *14*

3. Description of Scope of Work and Approach Taken **16**

3.1 Assessor's validation of defined cardholder data environment and scope accuracy *16*

3.2 Cardholder Data Environment (CDE) overview *17*

3.3 Network segmentation *17*

3.4 Network segment details *19*

3.5 Connected entities for payment processing and transmission *20*

3.6 Other business entities that require compliance with the PCI DSS *20*

3.7 Wireless summary *21*

3.8 Wireless details *21*

4. Details about Reviewed Environment **22**

4.1 Detailed network diagram(s) *22*

4.2 Description of cardholder data flows *24*

4.3 Cardholder data storage *26*

4.4 Critical hardware and software in use in the cardholder data environment *26*

4.5 Sampling… *27*

4.6 Sample sets for reporting *28*

4.7 Service providers and other third parties with which the entity shares cardholder data or that could affect the security of cardholder data *29*

4.8 Third-party payment applications/solutions *30*

4.9 Documentation reviewed *30*

4.10 Individuals interviewed *37*

4.11 Managed service providers *37*

4.12 Disclosure summary for "In Place with Compensating Control" responses *38*

4.13 Disclosure summary for "Not Tested" responses *38*

5. Quarterly Scan Results 39
5.1 Quarterly scan results 39
5.2 Attestations of scan compliance 40
6. Findings and Observations 41
Build and Maintain a Secure Network and Systems 41
Requirement 1: Install and maintain a firewall configuration to protect cardholder data 41
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 57
Protect Stored Cardholder Data 72
Requirement 3: Protect stored cardholder data 72
Requirement 4: Encrypt transmission of cardholder data across open, public networks 94
Maintain a Vulnerability Management Program 101
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs 101
Requirement 6: Develop and maintain secure systems and applications 109
Implement Strong Access Control Measures 140
Requirement 7: Restrict access to cardholder data by business need to know 140
Requirement 8: Identify and authenticate access to system components 148
Requirement 9: Restrict physical access to cardholder data 172
Regularly Monitor and Test Networks 195
Requirement 10: Track and monitor all access to network resources and cardholder data 195
Requirement 11: Regularly test security systems and processes 224
Maintain an Information Security Policy 242
Requirement 12: Maintain a policy that addresses information security for all personnel 242
Appendix A: Additional PCI DSS Requirements 265
Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers 266
Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections 270
Appendix A3: Designated Entities Supplemental Validation (DESV) 273
Appendix B: Compensating Controls 274
Appendix C: Compensating Controls Worksheet 275
Appendix D: Segmentation and Sampling of Business Facilities/System Components 277

Introduction to the ROC Template

This document, the *PCI DSS Template for Report on Compliance for use with PCI DSS v3.2.1, Revision 1.0* ("ROC Reporting Template"), is the mandatory template for Qualified Security Assessors (QSAs) completing a Report on Compliance (ROC) for assessments against the *PCI DSS Requirements and Security Assessment Procedures v3.2.1.* The ROC Reporting Template provides reporting instructions and the template for QSAs to use. This can help provide reasonable assurance that a consistent level of reporting is present among assessors.

Use of this Reporting Template is mandatory for all v3.2.1 submissions.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase/decrease the number of rows, or to change column width. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as the report is written and for the recipient in understanding the context the responses and conclusions are made. Addition of text or sections is applicable within reason, as noted above. Refer to the "Frequently Asked Questions for use with ROC Reporting Template for PCI DSS v3.x" document on the PCI SSC website for further guidance.

The Report on Compliance (ROC) is produced during onsite PCI DSS assessments as part of an entity's validation process. The ROC provides details about the entity's environment and assessment methodology, and documents the entity's compliance status for each PCI DSS Requirement. A PCI DSS compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The ROC is effectively a ***summary of evidence*** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROC provides a comprehensive ***summary of testing activities performed and information collected*** during the assessment against the *PCI DSS Requirements and Security Assessment Procedures v3.2.1*. The information contained in a ROC must provide enough detail and coverage to verify that the assessed entity is compliant with all PCI DSS requirements.

ROC Sections

The ROC includes the following sections and appendices:

- Section 1: Contact Information and Report Date
- Section 2: Summary Overview
- Section 3: Description of Scope of Work and Approach Taken
- Section 4: Details about Reviewed Environment
- Section 5: Quarterly Scan Results
- Section 6: Findings and Observations

- Appendix A: Additional PCI DSS Requirements
- Appendices B and C: Compensating Controls and Compensating Controls Worksheet (as applicable)
- Appendix D: Segmentation and Sampling of Business Facilities/System Components (diagram)

The first five sections must be thoroughly and accurately completed, in order for the assessment findings in Section 6 and any applicable responses in the Appendices to have the proper context. The Reporting Template includes tables with Reporting Instructions built-in to help assessors provide all required information throughout the document. Responses should be specific, but efficient. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage. Parroting the testing procedure within a description is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is discouraged and details should be specifically relevant to the assessed entity.

ROC Summary of Assessor Findings

With the Reporting Template, an effort was made to efficiently use space, and as such, there is one response column for results/evidence ("ROC Reporting Details: Assessor's Response") instead of three. Additionally, the results for "Summary of Assessor Findings" were expanded to more effectively represent the testing and results that took place, which should be aligned with the Attestation of Compliance (AOC).

There are now five results possible – In Place, In Place with CCW (Compensating Control Worksheet), Not Applicable, Not Tested, and Not in Place. At each sub-requirement there is a place to designate the result ("Summary of Assessor Findings"), which can be checked as appropriate. See the example format on the following page, as referenced.

The following table is a helpful representation when considering which selection to make. Remember, only one response should be selected at the sub-requirement level, and reporting of that should be consistent with other required documents, such as the AOC.

Refer to the "Frequently Asked Questions for use with ROC Reporting Template for PCI DSS v3.x" document on the PCI SSC website for further guidance.

RESPONSE	WHEN TO USE THIS RESPONSE:	USING THE SAMPLE BELOW:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.	*In the sample, the Summary of Assessment Findings at 1.1 is "in place" if all report findings are in place for 1.1.a and 1.1.b or a combination of in place and not applicable.*

RESPONSE	WHEN TO USE THIS RESPONSE:	USING THE SAMPLE BELOW:
In Place w/ CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.	*In the sample, the Summary of Assessment Findings at 1.1 is "in place with CCW" if all report findings are in place for 1.1.a and 1.1.b with the use of a CCW for one or both (completed at the end of the report) or a combination of in place with CCW and not applicable.*
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.	*In the sample, the Summary of Assessment Findings at 1.1 is "not in place" if either 1.1.a or 1.1.b are concluded to be "not in place."*
N/A (Not Applicable)	The requirement does not apply to the organization's environment. All "not applicable" responses require reporting on testing performed to confirm the "not applicable" status. Note that a "Not Applicable" response still requires a detailed description explaining how it was determined that the requirement does not apply. In scenarios where the Reporting Instruction states, "If 'no/yes', mark as Not Applicable," assessors may simply enter "Not Applicable" or "N/A" and are not required to report on the testing performed to confirm the "Not Applicable" status. **Certain requirements are always applicable (3.2.1-3.2.3, for example), and that will be designated by a grey box under "Not Applicable."**	*In the sample, the Summary of Assessment Findings at 1.1 is "not applicable" if both 1.1.a and 1.1.b are concluded to be "not applicable." A requirement is applicable if any aspects of the requirement apply to the environment being assessed, and a "Not Applicable" designation in the Summary of Assessment Findings should not be used in this scenario.* ***Note, future-dated requirements are considered Not Applicable until the future date has passed. While it is true that the requirement is likely not tested (hence the original instructions), it is not required to be tested until the future date has passed, and the requirement is therefore not applicable until that date. As such, a "Not Applicable" response to future-dated requirements is accurate, whereas a "Not Tested" response would imply there was not any consideration as to whether it could apply (and be perceived as a partial or incomplete ROC).* *Once the future date has passed, responses to those requirements should be consistent with instructions for all requirements.*

RESPONSE	WHEN TO USE THIS RESPONSE:	USING THE SAMPLE BELOW:
Not Tested	The requirement (or any single aspect of the requirement) was not included for consideration in the assessment and was not tested in any way. (See "What is the difference between 'Not Applicable' and 'Not Tested'?" in the following section for examples of when this option should be used.)	*In the sample, the Summary of Assessment Findings at 1.1 is "not tested" if either 1.1.a or 1.1.b are concluded to be "not tested."*

What is the difference between "Not Applicable" and "Not Tested?"

Requirements that are deemed to be not applicable to an environment must be verified as such. Using the example of wireless and an organization that does not use wireless technology in any capacity, an assessor could select "N/A" for Requirements 1.2.3, 2.1.1, and 4.1.1, after the assessor confirms that there are no wireless technologies used in their CDE or that connect to their CDE via assessor testing. Once this has been confirmed, the organization may select "N/A" for those specific requirements, and the accompanying reporting must reflect the testing performed to confirm the not applicable status.

If a requirement is completely excluded from review without any consideration as to whether it could apply, the "Not Tested" option should be selected. Examples of situations where this could occur may include:

- An organization may be asked by their acquirer to validate a subset of requirements—for example: using the prioritized approach to validate certain milestones.
- An organization may wish to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption methodology that requires assessment of PCI DSS Requirements 2, 3, and 4.
- A service provider organization might offer a service that covers only a limited number of PCI DSS requirements—for example, a physical storage provider may only wish to validate the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization only wishes to validate certain PCI DSS requirements even though other requirements might also apply to their environment. Compliance is determined by the brands and acquirers, and the AOCs they see will be clear in what was tested and not tested. They will decide whether to accept a ROC with something "not tested," and the QSA should speak with them if any exception like this is planned. This should not change current practice, just reporting.

Requirement X: Sample

Note – checkboxes have been added to the "Summary of Assessment Findings" so that the assessor may double click to check the applicable summary result. Hover over the box you'd like to mark and click once to mark with an 'x'. To remove a mark, hover over the box and click again.

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.1 Sample sub-requirement			☐	☐	☐	☐	☐
1.1.a Sample testing procedure	Reporting Instruction	*<Report Findings Here>*					
1.1.b Sample testing procedure	Reporting Instruction	*<Report Findings Here>*					

ROC Reporting Details

The reporting instructions in the Reporting Template explain the intent of the response required. There is no need to repeat the testing procedure or the reporting instruction within each assessor response. As noted earlier, responses should be specific and relevant to the assessed entity. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage and should avoid parroting of the testing procedure without additional detail or generic template language.

Assessor responses will generally fall into categories such as the following:

- One word **(yes/no)**

  Example Reporting Instruction: ***Indicate whether*** *the assessed entity is an issuer or supports issuing services.* ***(yes/no)***

- Document name or interviewee job title/reference – In Sections 4.9, "Documentation Reviewed," and 4.10, "Individuals Interviewed" below, there is a space for a reference number and ***it is the QSA's choice*** to use the document name/interviewee job title or the reference number at the individual reporting instruction response.

  Example Reporting Instruction: ***Identify*** *the document that defines vendor software development processes.*

  Example Reporting Instruction: ***Identify the individuals*** *interviewed who confirm that …*

- Sample description – For sampling, the QSA must use the table at "Sample sets for reporting" in the Details about Reviewed Environment section of this document to fully report the sampling, but ***it is the QSA's choice*** to use the Sample set reference number ("Sample Set-5") or list out the items from the sample again at the individual reporting instruction response. If sampling is not used, then the types of components that were tested must still be identified in Section 6 Findings and Observations. This may be accomplished by either using Sample Set Reference numbers or by listing the tested items individually in the response.

  Example Reporting Instruction: ***Identify the sample*** *of removable media observed.*

- Brief description/short answer – Short and to the point, but provide detail and individual content that is not simply an echoing of the testing procedure or reporting instruction nor a template answer used from report-to-report, but instead relevant and specific to the assessed entity. These responses must include unique details, such as the specific system configurations reviewed (to include what the assessor observed in the configurations) and specific processes observed (to include a summary of what was witnessed and how that verified the criteria of the testing

procedure). It is not enough to simply state that it was verified. Responses must go beyond that and include details regarding *how* a requirement is in place.

Example Reporting Instruction: ***Describe*** *the procedures for secure key distribution that were observed to be implemented.*

Example Reporting Instruction: For the interview, ***summarize the relevant details*** *discussed that verify …*

Dependence on another service provider's compliance:

Generally, when reporting on a requirement where a third-party service provider is responsible for the tasks, an acceptable response for an "in place" finding may be something like:

"Assessor verified this is the responsibility of Service Provider X, as verified through review of x/y contract (document). Assessor reviewed the AOC for Service Provider X, dated MM/DD/YYYY, and confirmed the service provider was found to be PCI DSS compliant ***against PCI DSS v3.2 (or PCI DSS v3.2.1)*** *for all applicable requirements, and that it covers the scope of the services used by the assessed entity."*

That response could vary, but what's important is that it is noted as "in place" and that there has been a level of testing by the assessor to support the conclusion that this responsibility is verified and that the responsible party has been tested against the requirement and found to be compliant.

Do's and Don'ts: Reporting Expectations

DO:	*DON'T:*
▪ Use this Reporting Template when assessing against v3.2.1 of the PCI DSS. ▪ Complete all sections in the order specified. ▪ Read and understand the intent of each Requirement and Testing Procedure. ▪ Provide a response for every Testing Procedure. ▪ Provide sufficient detail and information to support the designated finding, but be concise. ▪ Describe *how* a Requirement is in place per the Reporting Instruction, not just that it *was* verified. ▪ Ensure the parts of the Testing Procedure and Reporting Instruction are addressed. ▪ Ensure the response covers all applicable system components. ▪ Perform an internal quality assurance review of the ROC for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don't report items in the "In Place" column unless they have been verified as being "in place" as stated. ▪ Don't include forward-looking statements or project plans in the "In Place" assessor response. ▪ Don't simply repeat or echo the Testing Procedure in the response. ▪ Don't copy responses from one Testing Procedure to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment. ▪ Don't leave any spaces blank. If a section does not apply, annotate it as such.

ROC Template for PCI Data Security Standard v3.2.1

This template is to be used for creating a Report on Compliance. Content and format for a ROC is defined as follows:

1. Contact Information and Report Date

1.1 Contact information

Client	
▪ Company name:	Fairfax Imaging, Inc. (“Fairfax”)
▪ Company address:	2005 Pan Am Circle Suite 110, Tampa, FL 33607
▪ Company URL:	www.fairfaximaging.com
▪ Company contact name:	Nadine Chahal
▪ Contact phone number:	1-877-627-8325
▪ Contact e-mail address:	nadine.chahal@ffximg.com
Assessor Company	
▪ Company name:	360 Advanced, Inc. (“360 Advanced”)
▪ Company address:	200 Central Ave., Suite 2100 St. Petersburg, FL 33701
▪ Company website:	http://www.360advanced.com
Assessor	
▪ Lead Assessor name:	Phillip Hagan
▪ Assessor PCI credentials: (QSA, PA-QSA, etc.)	QSA 204-876
▪ Assessor phone number:	1-866-418-1708
▪ Assessor e-mail address:	phagan@360advanced.com
▪ List all other assessors involved in the assessment. If there were none, mark as Not Applicable. (add rows as needed)	
Assessor name:	Assessor PCI credentials: (QSA, PA-QSA, etc.)
Not Applicable	Not Applicable
▪ List all Associate QSAs involved in the assessment. If there were none, mark as Not Applicable. (add rows as needed)	
Associate QSA name:	Associate QSA mentor name:
Not Applicable	Not Applicable

Assessor Quality Assurance (QA) Primary Reviewer for this specific report (not the general QA contact for the QSA)	
▪ QA reviewer name:	Virgil Floresca, PCI QSA 203-736
▪ QA reviewer phone number:	1-866-418-1708
▪ QA reviewer e-mail address:	vfloresca@360advanced.com

1.2 Date and timeframe of assessment

▪ Date of Report:	December 8, 2021
▪ Timeframe of assessment (start date to completion date):	June 8, 2021 – December 8, 2021
▪ Identify date(s) spent onsite at the entity:	July 8, 2021 – August 5, 2021 360 Advanced performed remote assessments via virtual walkthroughs, demonstrations, and interviews throughout the specified timeframe of the engagement due to the COVID-19 pandemic.
▪ Describe the time spent onsite at the entity, time spent performing remote assessment activities and time spent on validation of remediation activities.	During the virtual walkthroughs conducted on the above dates, the following activities were performed: **Inquiry / Interview** – Inquired of appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➢ Knowledge and additional information regarding the policy or procedure; and ➢ Corroborating evidence of the policy or procedure. **Inspection** – Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ➢ Examination / Inspection of source documentation and authorizations to verify transactions processed; ➢ Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures; ➢ Examination / Inspection of systems documentation, configurations and settings; and ➢ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions. NOTE – inspections of systems and evidence also occurred remotely to prepare for onsite and to finish out testing. **Observation** – Observed the implementation, application or existence of specific controls as represented

1.3 PCI DSS version

▪ Version of the PCI Data Security Standard used for the assessment (should be 3.2.1):	3.2.1

1.4 Additional services provided by QSA company

The PCI SSC Qualification Requirements for Qualified Security Assessors (QSA) v3.0 includes content on "Independence," which specifies requirements for assessor disclosure of services and/or offerings that could reasonably be viewed to affect independence of assessment. Complete the below after review of relevant portions of the Qualification Requirements document(s) to ensure responses are consistent with documented obligations.

▪ Disclose all services offered to the assessed entity by the QSAC, including but not limited to whether the assessed entity uses any security-related devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights or that the QSA has configured or manages:	Technology audit, IT assurance, and compliance services. Specifically: Penetration Testing, PCI-DSS assessment, and SOC 2 examinations.
▪ Describe efforts made to ensure no conflict of interest resulted from the above mentioned services provided by the QSAC:	360 Advanced did not provide services that could affect the independence of the assessment performed, or that could constitute a conflict of interest. 360 Advanced is engaged to conduct other assessment / examination services including, penetration testing and SOC 2 but is not providing consulting or selling of any tools.

1.5 Summary of Findings

PCI DSS Requirement	Summary of Findings (check one)			
	Compliant	Non-Compliant	Not Applicable	Not Tested
1. Install and maintain a firewall configuration to protect cardholder data	☒	☐	☐	☐
2. Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	☐	☐
3. Protect stored cardholder data	☒	☐	☐	☐
4. Encrypt transmission of cardholder data across open, public networks	☒	☐	☐	☐
5. Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	☐	☐
6. Develop and maintain secure systems and applications	☒	☐	☐	☐
7. Restrict access to cardholder data by business need to know	☒	☐	☐	☐
8. Identify and authenticate access to system components	☒	☐	☐	☐
9. Restrict physical access to cardholder data	☒	☐	☐	☐
10. Track and monitor all access to network resources and cardholder data	☒	☐	☐	☐
11. Regularly test security systems and processes	☒	☐	☐	☐
12. Maintain a policy that addresses information security for all personnel	☒	☐	☐	☐
Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	☒	☐
Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections	☐	☐	☒	☐
Appendix A3: Designated Entities Supplemental Validation	☐	☐	☒	☐

2. Summary Overview

2.1 Description of the entity's payment card business

Provide an overview of the entity's payment card business, including:

▪ Describe the nature of the entity's business (what kind of work they do, etc.) ***Note:*** *This is not intended to be a cut-and-paste from the entity's website, but should be a tailored description that shows the assessor understands the business of the entity being assessed.*	Fairfax Software provides workflow services via document imaging and automated data capture solutions to facilitate secure customer payments for their clients. Quick Cashier processes in-person credit card payments. Quick Modules converts physical forms to a digital copy to extract relevant payment fields using recognition technology.
▪ Describe how the entity stores, processes, and/or transmits cardholder data. ***Note:*** *This is not intended to be a cut-and-paste from above, but should build on the understanding of the business and the impact this can have upon the security of cardholder data.*	**Transmission of potential CHD** The Fairfax Quick Modules flow of cardholder data begins with the receipt of payment authorization forms as paper material. This form is then scanned into a designated Fairfax workstation using an assigned Quick Modules scanner device for temporary storage. The image of the form is directly uploaded to the Quick Modules platform hosted solely within Amazon Web Services cloud environment. This image file is securely transferred using TLS v1.2. Quick Cashier is the front-end web application on the client-owned cashier workstations. QuickCashier interfaces with client middleware which in turn communicates with the Point-of-Sale device APIs to facilitate the credit card swipe. QuickCashier also allows for manual entry of the credit card by a cashier. The client middleware performs the CC encryption / decryption process by receiving the encrypted credit card data from the POS device and passing it to the description service via HTTPS and receiving back the decrypted CC data. The decrypted CC data is sent to the client-selected payment gateway for tokenization via HTTPS. Next the CC token and line-item information is sent to the payment gateway via HTTPS to assess fees. After the customer accepts the charges the CC token is submitted via HTTPS to the payment gateway for processing. Once the payment is processed the payment summary is sent to QuickCashier to complete the cashiering transaction. Communication between the QuickCashier front end and any client middleware is completed utilizing a web service local call via Java-script. **Processing of CHD** The flow of information scanned from a paper authorization form is as follows: ➢ The Quick Modules platform receives the image potentially containing CHD and stores it in an encrypted EBS volume

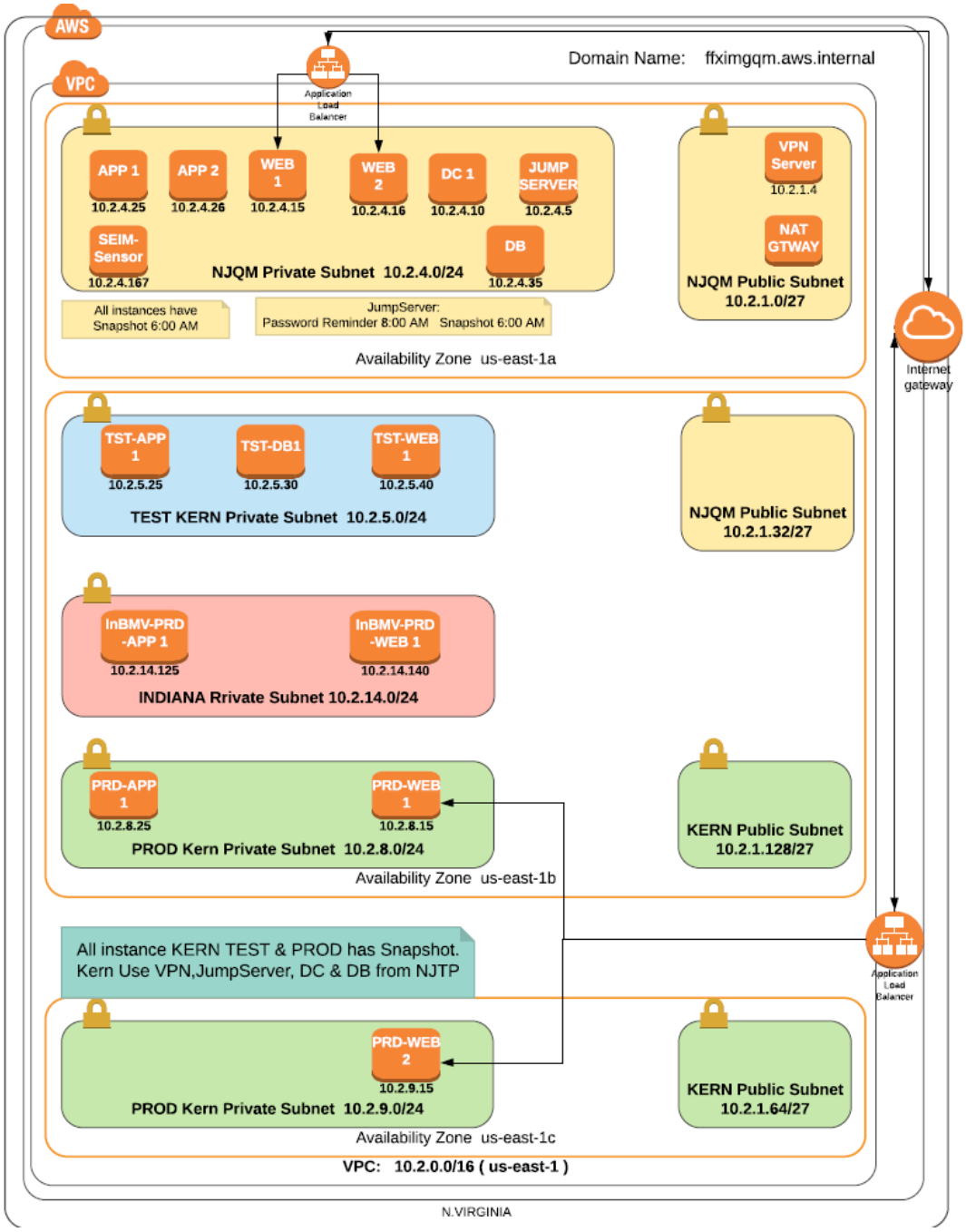
	➢ The image is run through the Quick Modules' Optical Character Recognition (OCR) engine where potential CHD is extracted and stored within a database residing in an encrypted EBS volume ➢ Reporting output of potential CHD is determined by the client and then exchanged using a secure method via either SFTP or HTTPS ➢ Clients will then process payments though their own payment processors. This is independent from Fairfax's own payment services such as Quick Payments and is deemed out of scope of this assessment. Processing of CC information for Quick Cashier is handled via the client middleware transmissions utilizing HTTPS to and from a third-party (Fidelity Information Services (FIS)) payment gateway. **Storage of potential Cardholder Data** Storage of Quick Modules cardholder data is potentially in the form of both hard copy material and electronic media. Hard copy material potentially containing CHD printed or written on payment authorization forms are stored securely within a data processing room located within the Fairfax office in Tampa, FL while electronic copies and extracted CHD are stored encrypted within the cloud-hosted environment at AWS. Storage of QuickCashier data is the tokenized CC information and any related cashiering transaction details returned by the FIS payment gateway.
▪ Describe why the entity stores, processes, and/or transmits cardholder data. ***Note:*** *This is not intended to be a cut-and-paste from above, but should build on the understanding of the business and the impact this can have upon the security of cardholder data.*	Fairfax potentially receives, stores, and transmits CHD as a requirement of its services being provided. No processing of payments is performed directly by Fairfax. Output of CHD is provided to clients to be processed by their own payment processors.

▪ Identify the types of payment channels the entity serves, such as card-present and card-not-present (for example, mail order/telephone order (MOTO), e-commerce).	Fairfax does not process payments on behalf of the client. Output files potentially containing the extracted CHD from paper authorization forms are provided by Quick Modules to clients to be processed by their own payment processors. Fairfax serves both card-present and card-not-present channels. Card-present transactions are supported via point-of-sale devices and manual entry by a cashier. Client systems utilizing software that interfaces with the point of sale devices handle any credit card processing and are out of scope as they are vetted to secure the transaction from end to end and only pass the tokenized data to Quick Cashier. Manual entry of the CC information is completed by the cashier directly into the Quick Cashier web application. It is the responsibility of Fairfax clients to manage and secure these devices as indicated within requirement nine. Fairfax did not operate, manage, or maintain any devices that capture payment card data via direct physical interaction. Card not present transactions occur when physical payment authorization forms potentially containing CHD are scanned and converted into a digital copy to extract relevant payment fields using recognition technology. Any potential credit card information is then processed to provide an output file in a format defined by the client. This file is then uploaded to a client-specified source using a secure method (either HTTPS or SFTP). This provides an automated process for data entry of credit card information into the Fairfax payment page web fields. No magnetic stripe or PIN information is stored or sent to the application itself.
▪ Other details, if applicable:	None noted.

2.2 High-level network diagram(s)

Provide a ***high-level*** network diagram (either obtained from the entity or created by assessor) of the entity's networking topography, showing the overall architecture of the environment being assessed. This high-level diagram should summarize all locations and key systems, and the boundaries between them and should include the following:

- Connections into and out of the network including demarcation points between the cardholder data environment (CDE) and other networks/zones
- Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
- Other necessary payment components, as applicable



3. Description of Scope of Work and Approach Taken

3.1 Assessor's validation of defined cardholder data environment and scope accuracy

Document how the assessor validated the accuracy of the defined CDE/PCI DSS scope for the assessment, including:

As noted in PCI DSS, v3.2.1 – "At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or if compromised could impact the CDE (e.g. authentication servers) to ensure they are included in the PCI DSS scope." *Note – additional reporting has been added below to emphasize systems that are connected to or if compromised could impact the CDE.*	
▪ Describe the methods or processes (for example, the specific types of tools, observations, feedback, scans, data flow analysis) used to identify and document all existences of cardholder data (as executed by the assessed entity, assessor or a combination):	360 Advanced inspected the network and data-flow diagrams in conjunction with vulnerability scans and penetration testing reports to verify that systems and network components where cardholder data flows, or systems are connected, were documented, and assessed. A demonstration of the process flow was observed to validate the input of cardholder data through the scanning process and secure transmission of data to the cloud environment and the final output transmission to the client.
▪ Describe the methods or processes (for example, the specific types of tools, observations, feedback, scans, data flow analysis) used to verify that no cardholder data exists outside of the defined CDE (as executed by the assessed entity, assessor or a combination):	360 Advanced inspected network and data-flow diagrams in conjunction with vulnerability scans and pen testing reports to verify the entry and exit points of cardholder data within the CDE scope defined for this assessment.
▪ Describe how the results of the methods/processes were documented (for example, the results may be a diagram or an inventory of cardholder data locations):	360 Advanced validated the scope of the assessment through interviews with several subject matter experts (SME), analysis of security groups and network / data-flow diagrams, and review of vulnerability assessments and penetration testing reports.
▪ Describe how the results of the methods/processes were evaluated by the assessor to verify that the PCI DSS scope of review is appropriate: ***Note** – the response must go beyond listing the activities that the assessor performed to evaluate the results of the methods/processes; the assessor must also include details regarding the results of the outcome of those activities that gave the assessor the level of assurance that the scope is appropriate.*	The results of the above methods / processes were documented as inventory listings, network diagrams, third-party report results, and configuration files for the network components deemed in scope.
▪ Describe why the methods (for example, tools, observations, feedback, scans, data flow analysis, or any environment design decisions that were made to help limit the scope of the environment) used for scope verification are considered by the assessor to be effective and accurate:	The above methods used for scope verification are considered to be effective and accurate due to the multiple layers of validation performed via inquiry, inspection, and observations.
▪ Provide the name of the assessor who attests that the defined CDE and scope of the assessment has been verified to be accurate, to the best of the assessor's ability and with all due diligence:	Phillip Hagan, QSA # 203-736

▪ Other details, if applicable:	None noted.

3.2 Cardholder Data Environment (CDE) overview

Provide an overview of the cardholder data environment encompassing the people, processes, technologies, and locations (for example, client's Internet access points, internal corporate network, processing connections).

▪ People – such as technical support, management, administrators, operations teams, cashiers, telephone operators, physical security, etc.: ***Note** – this is not intended to be a list of individuals interviewed, but instead a list of the types of people, teams, etc. who were included in the scope.*	Senior management, Information Technology, Human Resources, and software development personnel.
▪ Processes – such as payment channels, business functions, etc.:	Secure transmission and storage of CHD, software development procedures, user access management, configuration management, and vulnerability management procedures, incident response procedures.
▪ Technologies – such as e-commerce systems, internal network segments, DMZ segments, processor connections, POS systems, encryption mechanisms, etc.: ***Note** – this is not intended to be a list of devices but instead a list of the types of technologies, purposes, functions, etc. included in the scope.*	Segmentation technologies – AWS Security Groups, AWS Virtual Private Cloud, Bastion Host / Jump Server Virtualization technologies – AWS EC2 Security technologies – Intrusion Detection Systems, File Integrity Monitoring, Anti-virus, Centralized Logging, Multi-Factor Authentication, Web Application Firewall
▪ Locations/sites/stores – such as retail outlets, data centers, corporate office locations, call centers, etc.:	The cardholder data environment was scoped and limited to system components hosted within the AWS cloud environment.
▪ Other details, if applicable:	Not applicable

3.3 Network segmentation

▪ Identify whether the assessed entity has used network segmentation to reduce the scope of the assessment. **(yes/no)** ***Note** -- An environment with no segmentation is considered a "flat" network where all systems are considered in scope due to a lack of segmentation.*	Yes
▪ ***If segmentation is not used:*** Provide the name of the assessor who attests that the whole network has been included in the scope of the assessment.	Not applicable

▪ ***If segmentation is used:*** Briefly describe how the segmentation is implemented.	A variety of segmentation technologies using AWS security groups, network access control lists, NAT, and integrated routing / switching technologies was implemented to restrict and limit access to the CDE. In addition, only authorized individuals were able to remote into the environment via SSH using a jump server / bastion host that implemented multi-factor network authentication.
– Identify the technologies used and any supporting processes	SSH bastion host implemented with multi-factor network authentication AWS Security Groups and NACLs
– Explain how the assessor validated the effectiveness of the segmentation, as follows:	
– Describe the methods used to validate the effectiveness of the segmentation (for example, observed configurations of implemented technologies, tools used, network traffic analysis, etc.).	360 Advanced validated the effectiveness of the segmentation by inspecting AWS instance configurations in comparison to network and data flow diagrams. In addition, output of penetration tests and vulnerability scans were inspected to further provide evidence of the effectiveness of the segmentation technologies in place.
– Describe how it was verified that the segmentation is functioning as intended ***Note –*** *the response must go beyond listing the activities that the assessor performed and must provide specific details regarding how segmentation is functioning as intended.*	360 Advanced verified that the segmentation was functioning as intended by performing ping, traceroute, and telnet commands from the corporate office environment to verify isolation between known segments of the network. Internal and external penetration tests and vulnerability scan reports were also inspected to verify that segmentation between security zones were properly configured.
– Identify the security controls that are in place to ensure the integrity of the segmentation mechanisms (e.g., access controls, change management, logging, monitoring, etc.).	360 Advanced verified that mechanisms were in place to ensure the integrity of the segmentation. A firewall change review process is in place. In addition, centralized logging is in place to allow monitoring and alerting on any suspicious network traffic flows.
– Describe how it was verified that the identified security controls are in place ***Note*** *– the response must go beyond listing the activities that the assessor performed and must provide specific details of what the assessor observed to get the level of assurance that the identified security controls are in place.*	360 Advanced verified that adequate security controls were in place to ensure the integrity of the segmentation mechanisms by evaluating both internal and external vulnerability scans that were conducted quarterly throughout the year. In addition, a yearly penetration test was performed to add evidence of the segmentation controls in place.
▪ Provide the name of the assessor who attests that the segmentation was verified to be adequate to reduce the scope of the assessment AND that the technologies/processes used to implement segmentation were included in the PCI DSS assessment.	Phillip Hagan, QSA # 203-736

3.4 Network segment details

Describe all networks that store, process and/or transmit CHD:

Network Name (in scope)	Function/ Purpose of Network
Fairfax's AWS hosted network	Secure network for Quick Modules Application services. Network is housed and maintained by AWS offsite from Fairfax's corporate office.
Data Processing network	Secure network connecting the scanner and scanning workstation at Fairfax's corporate office.

Describe all networks that do not store, process and/or transmit CHD, but are still in scope (e.g., connected to the CDE or provide management functions to the CDE):

Network Name (in scope)	Function/ Purpose of Network
Bastion host network	Provides a single point of access for management within the CDE. SSH access is only granted via multi-factor network authentication. Bastion host network

Describe any networks confirmed to be out of scope:

Network Name (out of scope)	Function/ Purpose of Network
Corporate office	Network is used only to facilitate access to web applications and VPN if access granted.
VM Farms and AWS non-CDE networks	VM Farms and AWS provides the hosting environments for Fairfax's applications and services outside of the CDE.

3.5 Connected entities for payment processing and transmission

Complete the following for connected entities for processing and/or transmission. If the assessor needs to include additional reporting for the specific brand and/or acquirer, it can be included either here within 3.5 or as an appendix at the end of this report. Do not alter the Attestation of Compliance (AOC) for this purpose.

Identify All Processing and Transmitting Entities (i.e. Acquirer/ Bank/ Brands)	Directly Connected? (yes/no)	Reason(s) for Connection:		Description of any discussions/issues between the QSA and Processing Entity on behalf of the Assessed Entity for this PCI DSS Assessment (if any)
		Processing	Transmission	
Not applicable		☐	☐	Not applicable

▪ Other details, if applicable (add content or tables here for brand/acquirer use, if needed):	Not applicable

3.6 Other business entities that require compliance with the PCI DSS

Entities wholly owned by the assessed entity that are required to comply with PCI DSS:

(This may include subsidiaries, different brands, DBAs, etc.)

Wholly Owned Entity Name	Reviewed:	
	As part of this assessment	Separately
Not applicable	Not applicable	Not applicable

International entities owned by the assessed entity that are required to comply with PCI DSS:

List all countries where the entity conducts business. (If there are no international entities, then the country where the assessment is occurring should be included at a minimum.)	Country
	United States of America

International Entity Name	Facilities in this country reviewed:	
	As part of this assessment	Separately
Not applicable	Not applicable	Not applicable

3.7 Wireless summary

▪ Indicate whether there are wireless networks or technologies in use (in or out of scope), **(yes/no)**	Wi-Fi technology is not utilized within the CDE which resides entirely on the AWS cloud environment.
If "no," describe how the assessor verified that there are no wireless networks or technologies in use.	Not applicable.
*If "yes," indicate whether wireless is in scope (i.e. part of the CDE, connected to or could impact the security of the cardholder data environment), **(yes/no)**:* This would include: – Wireless LANs – Wireless payment applications (for example, POS terminals) – All other wireless devices/technologies	Not applicable.

3.8 Wireless details

For each wireless technology in scope, identify the following:

Identified wireless technology	For each wireless technology in scope, identify the following (yes/no):		
	Whether the technology is used to store, process or transmit CHD	Whether the technology is connected to or part of the CDE	Whether the technology could impact the security of the CDE
Not applicable	Not applicable	Not applicable	Not applicable

Wireless technology not in scope for this assessment:

Identified wireless technology (not in scope)	Describe how the wireless technology was validated by the assessor to be not in scope
Not applicable	Not applicable

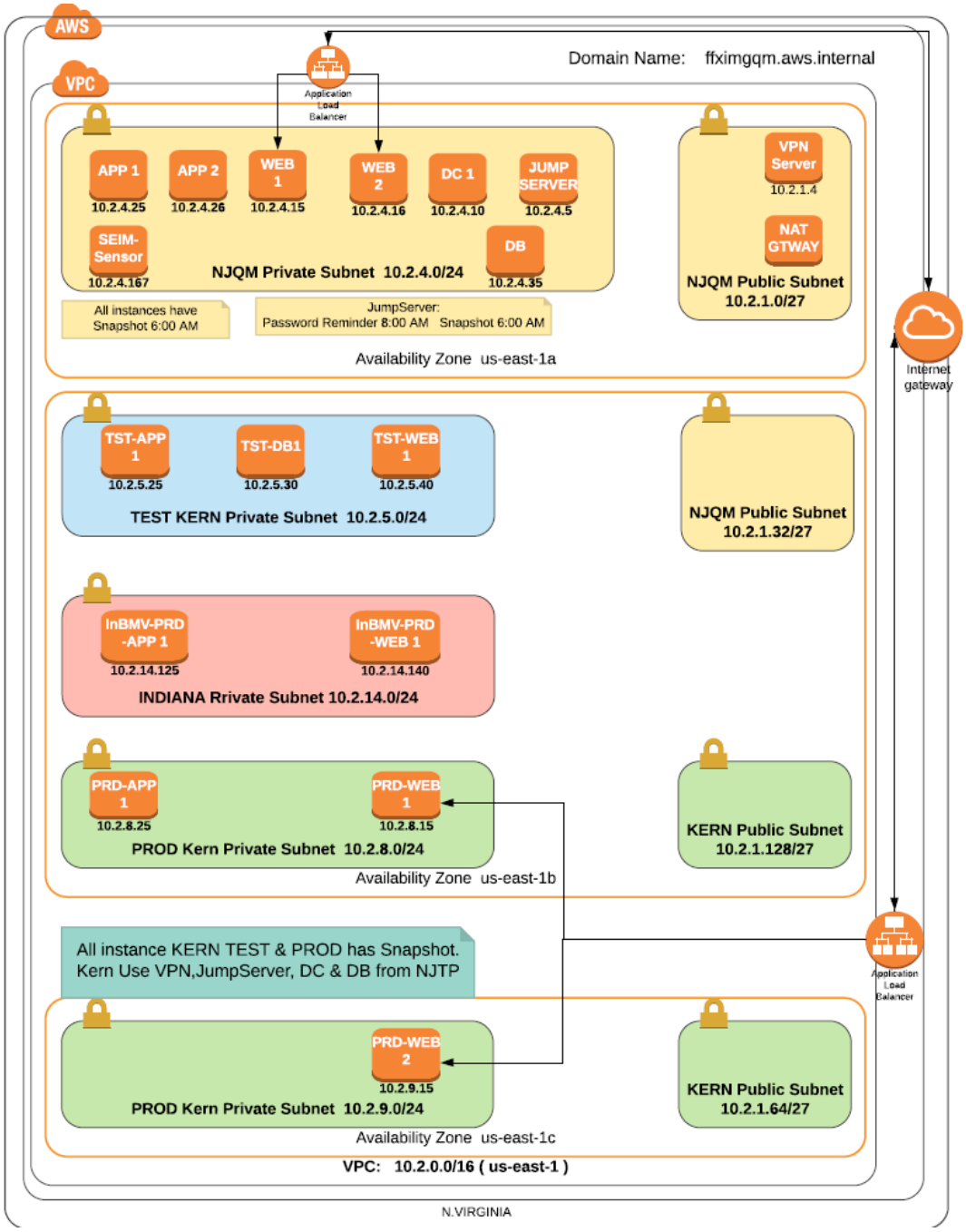
4. Details about Reviewed Environment

4.1 Detailed network diagram(s)

Provide one or more ***detailed diagrams*** to illustrate each communication/connection point between in scope networks/environments/facilities. Diagrams should include the following:

- All boundaries of the cardholder data environment
- Any network segmentation points which are used to reduce scope of the assessment
- Boundaries between trusted and untrusted networks
- Wireless and wired networks
- All other connection points applicable to the assessment

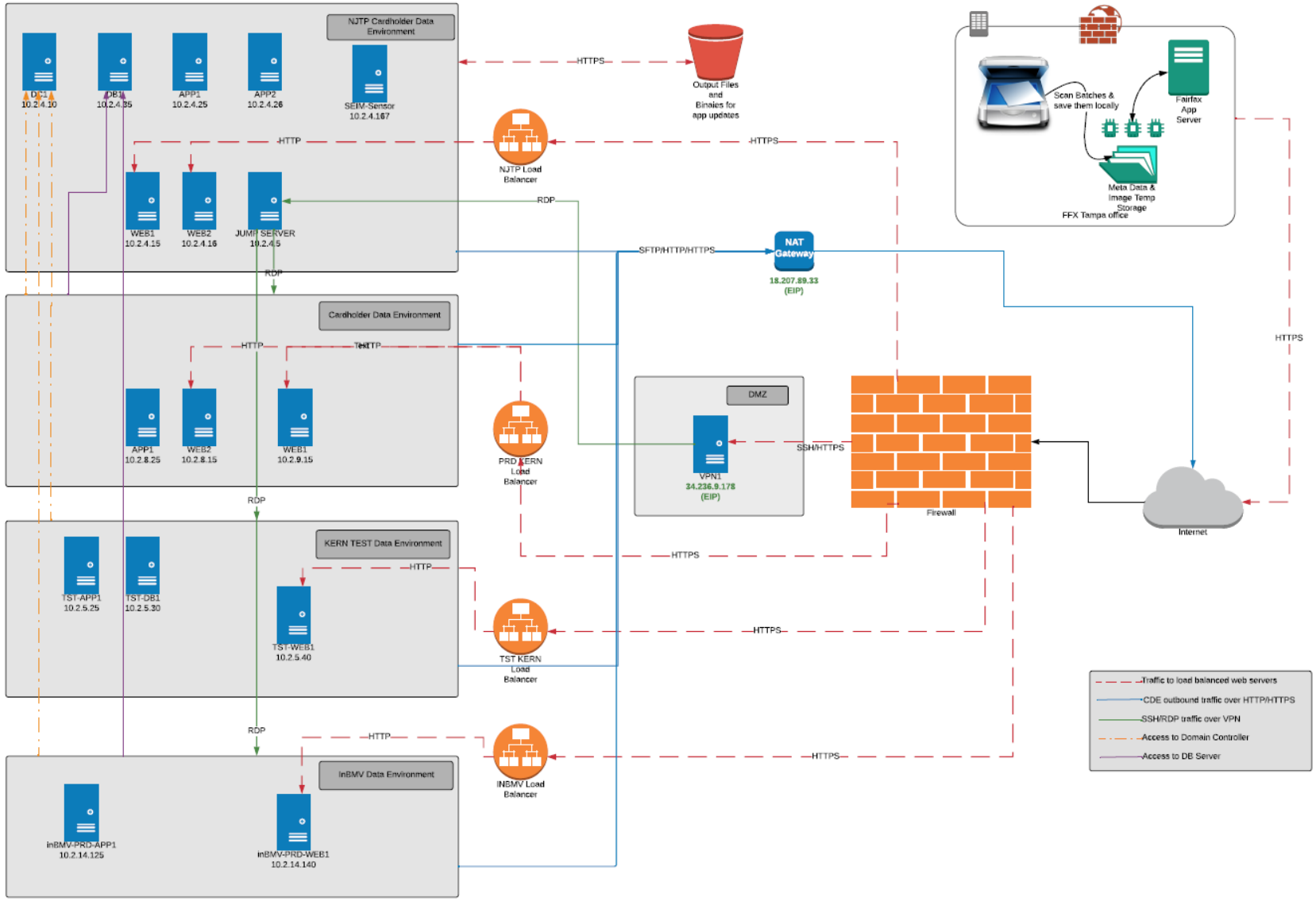
Ensure the diagram(s) include enough detail to clearly understand how each communication point functions and is secured. *(For example, the level of detail may include identifying the types of devices, device interfaces, network technologies, protocols, and security controls applicable to that communication point.)*



4.2 Description of cardholder data flows

Note: *The term "Capture" in Section 4.2 of the ROC Template refers to the specific transaction activity, while the use of "capture" in PCI DSS Requirement 9.9 refers to the receiving of cardholder data via physical contact with a payment card (e.g. via swipe or dip).*

Cardholder data-flow diagrams may also be included as a supplement to the description of how cardholder data is transmitted and/or processed.



Cardholder data flows	Types of CHD involved (for example, full track, PAN, expiry, etc.)	Describe how cardholder data is transmitted and/or processed and for what purpose it is used (for example, which protocols or technologies were used in each transmission)
Capture	PAN, expiry, and cardholder name	Payment forms are mailed to the Fairfax corporate office to be scanned within the secure data processing room. Images of the scanned material are securely transferred to the Quick Modules environment hosted in AWS. CHD is extracted from the images via OCR and a report generated based on a client-requested format. This report is then transferred to the client through a secure method (HTTPS or SFTP) they decide upon.
Authorization	Not applicable	Not applicable
Settlement	Not applicable	Not applicable
Chargeback	Not applicable	Not applicable
Identify all other data flows, as applicable (add rows as needed)		
Other (describe)		
Other details regarding the flow of CHD, if applicable:		

4.3 Cardholder data storage

Identify and list all databases, tables, and files storing post-authorization cardholder data and provide the following details.

Note: *The list of files and tables that store cardholder data in the table below must be supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers.*

Data Store (database, etc.)	**File(s) and/or Table(s)**	**Cardholder data elements stored** (for example, PAN, expiry, Name, any elements of SAD, etc.)	**How data is secured** (for example, what type of encryption and strength, hashing algorithm and strength, tokenization, access controls, truncation, etc.)	**How access to data stores is logged** (description of logging mechanism used for logging access to data—for example, describe the enterprise log management solution, application-level logging, operating system logging, etc. in place)
Database	Scanned image file CHD fields	PAN, expiry, and cardholder name	EBS encrypted volumes	Access is logged through both Windows audit policies and the Trend Micro logging agent.

4.4 Critical hardware and software in use in the cardholder data environment

Identify and list all types of hardware and critical software in the cardholder environment. Critical hardware includes network components, servers and other mainframes, devices performing security functions, end-user devices (such as laptops and workstations), virtualized devices (if applicable) and any other critical hardware – including homegrown components. Critical software includes e-commerce applications, applications accessing CHD for non-payment functions (fraud modeling, credit verification, etc.), software performing security functions or enforcing PCI DSS controls, underlying operating systems that store, process or transmit CHD, system management software, virtualization management software, and other critical software – including homegrown software/applications. For each item in the list, provide details for the hardware and software as indicated below. Add rows, as needed.

Critical Hardware			**Critical Software**		**Role/Functionality**
Type of Device (for example, firewall, server, IDS, etc.)	**Vendor**	**Make/Model**	**Name of Software Product**	**Version or Release**	
AWS Server Instances (Cloud-based)	Microsoft	Windows Server 2016 and 2019			Proxies, Application Servers, Web Servers, Database Servers, NAT services, and Infrastructure Management Servers
AWS Elastic Load Balancers	Amazon	AWS			Load Balancers
			AWS	N/A	Cloud infrastructure hosting the CDE

Critical Hardware			Critical Software		Role/Functionality
Type of Device (for example, firewall, server, IDS, etc.)	**Vendor**	**Make/Model**	**Name of Software Product**	**Version or Release**	
			McAfee LiveSafe	N/A	Workstation Anti-virus Software
			TrendMicro Deep Security	N/A	Security Automation Platform (IDS, FIM, Software Inventory, MFA, WAF, Log Monitoring, Log Analysis, Anti-malware) for servers
			Microsoft Windows	Server 2016 and 2019	Server Operating System

4.5 Sampling

Identify whether sampling was used during the assessment.

▪ If sampling is not used:	
– Provide the name of the assessor who attests that every system component and all business facilities have been assessed.	Not applicable
▪ If sampling is used:	
– Provide the name of the assessor who attests that all sample sets used for this assessment are represented in the below "Sample sets for reporting" table. *Examples may include, but are not limited to firewalls, application servers, retail locations, data centers, User IDs, people, etc.*	Phillip Hagan, QSA # 203-736
– Describe the sampling rationale used for selecting sample sizes (for people, processes, technologies, devices, locations/sites, etc.).	Sample sizes were selected first by obtaining the total population of evidence or equipment related to the requirement. A random sample was then selected and obtained using a randomization methodology that would provide a proper sample to appropriately meet 360 Advanced's sampling standards and provide a reasonable representation of the population when considering the maturity of associated processes in comparison to relevant risks. For servers and network devices, a sampling based off of functionality is performed upon review of inventories and inquiries confirming the scope of the CDE.
– If standardized PCI DSS security and operational processes/controls were used for selecting sample sizes, describe how they were validated by the assessor.	The above processes and controls were validated against network diagrams, data flow diagrams, and inventories of systems in scope

4.6 Sample sets for reporting

Note: *If sampling is used, this section MUST be completed. When a reporting instruction asks to identify a sample, the QSA may either refer to the Sample Set Reference Number (for example "Sample Set-1") OR list the sampled items individually in the response. Examples of sample sets may include, but are not limited to, firewalls, application servers, retail locations, data centers, User IDs, people, etc. Add rows as needed.*

Sample Set Reference Number	**Sample Type/ Description** (e.g., firewalls, datacenters, change records, User IDs, etc.)	**Listing of all items (devices, locations, change records, people, etc.) in the Sample Set**	**Make/Model of Hardware Components or Version/Release of Software Components**	**Total Sampled**	**Total Population**
Sample Set-1	Servers	APP1 DB1 DC1 JUMP-SERVER-NJQ WEB2 KRN-PRD-APP1 INBMV-PRD-APP1 INBMV-PRD-WEB1	AWS AMI based on Windows 2016 AWS AMI based on Windows 2019	8	15
Sample Set-2	Administrator Laptops	Alex Umansky - 5HNMJ52	Windows 10	1	2
Sample Set-3	New Hires	Gudimetla, Sowmya Hunter, Hayley Isabella Joyner, Anna Nicole Sabre, Daniel Edward Swearengin, Sophia Lynn Vawter, Loretta Rose Weisberg, Richard S	Not Applicable	7	15

Sample Set Reference Number	Sample Type/ Description (e.g., firewalls, datacenters, change records, User IDs, etc.)	Listing of all items (devices, locations, change records, people, etc.) in the Sample Set	Make/Model of Hardware Components or Version/Release of Software Components	Total Sampled	Total Population
Sample Set-4	Tenured Employees	Chahal, Alex Mohler, Michael T moliva, gaston Soto, Angela C Uehara, Ema Wells, Ashley N Wilcox, Stephen C.	Not Applicable	7	64
Sample Set-5	Terminated Employees	Rokhlin, Henry Hernandez, Richard A Mardini, Jamal Bates, Jasmine Renee Ferguson, John D	Not Applicable	5	9

4.7 Service providers and other third parties with which the entity shares cardholder data or that could affect the security of cardholder data

For each service provider or third party, provide:

Note: *These entities are subject to PCI DSS Requirement 12.8.*

Company Name	What data is shared (for example, PAN, expiry date, etc.)	The purpose for sharing the data (for example, third-party storage, transaction processing, etc.)	Status of PCI DSS Compliance (Date of AOC and version #)
Amazon Web Services	None	Cloud Service Provider for hosted application environment	Valid through June 30, 2022 on v3.2.1
Fidelity Information Services (FIS)	PAN, CVV, expiry date	Payment gateway provider used for tokenization and payment processing	Valid through March 31, 2022 on v3.2.1

4.8 Third-party payment applications/solutions

Use the table on the following page to identify and list all third-party payment application products and version numbers in use, including whether each payment application has been validated according to PA-DSS or PCI P2PE. Even if a payment application has been PA-DSS or PCI P2PE validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's *PA-DSS Implementation Guide* for PA-DSS applications *or P2PE Implementation Manual (PIM) and* P2PE application vendor's P2PE Application Implementation Guide for PCI P2PE applications/solutions.

Note: *It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.*

Note*: Homegrown payment applications/solutions* ***must*** *be reported at the section for Critical Hardware and Critical Software. It is also strongly suggested to address such homegrown payment applications/solutions below at "Any additional comments or findings" in order to represent all payment applications in the assessed environment in this table.*

Name of Third-Party Payment Application/Solution	Version of Product	PA-DSS validated? (yes/no)	P2PE validated? (yes/no)	PCI SSC listing reference number	Expiry date of listing, if applicable
Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
▪ Provide the name of the assessor who attests that all PA-DSS validated payment applications were reviewed to verify they have been implemented in a PCI DSS compliant manner according to the payment application vendor's PA-DSS Implementation Guide				Not applicable	
▪ Provide the name of the assessor who attests that all PCI SSC-validated P2PE applications and solutions were reviewed to verify they have been implemented in a PCI DSS compliant manner according to the P2PE application vendor's *P2PE Application Implementation Guide* and the P2PE solution vendor's *P2PE Instruction Manual (PIM).*				Not applicable	
▪ For any of the above Third-Party Payment Applications and/or solutions that are not listed on the PCI SSC website, identify any being considered for scope reduction/exclusion/etc.				Not applicable	
▪ Any additional comments or findings the assessor would like to include, as applicable:				Not applicable	

4.9 Documentation reviewed

Identify and list all reviewed documents. Include the following:

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
APP-01.3	Application - Encrypt Transmission of Sensitive Data	Evidence that sensitive data such as passwords and cardholder data are encrypted when transmitted from the in-scope application	06/2021

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
APP-01.4	Application Configuration - Encrypt Storage of Sensitive Data	Evidence that the in-scope application passwords are stored encrypted	06/2021
AS-01	Risk Assessment Result Documentation	Risk assessment documentation and report results	08/2021
AS-02.1	External & Internal Pen Test & Remediation	Annual penetration testing report and remediation of findings discovered	09/2021
AS-04.1	Incident Response Plan	Formal Incident Response Plan documentation indicated processes followed when an incident occurs	09/2021
AS-04.2	Incident Response Testing & Training	Incident response documentation indicating annual testing and training	08/2021
AV-01	Server AV - Running & Prevent Disabling	Evidence that anti-virus is running and cannot be disabled by the user	06/2021
AV-02	Server AV - Update Schedule	Anti-virus signature update settings for server endpoint protection	06/2021
AV-03	Server AV - Scan Schedule	Anti-virus scheduled scan settings	06/2021
AV-04	Server AV - Detection Action	Anti-virus settings indicating the action to be taken if a malicious file is detected	06/2021
AWS-01	AWS IAM - User Listing & Access Permissions & MFA	Amazon Web Services user listing and role permissions	06/2021
AWS-02	AWS IAM - Password Policy	Amazon Web Services Identity and Access Management password policy settings	06/2021
AWS-03	AWS VPC - Virtual Networking	Amazon Web Services network settings including VPC and VPN details	06/2021
AWS-04	AWS VPC - Security Groups	Amazon Web Services security groups and network access control lists bound to instances	06/2021
AWS-05	AWS EC2 - Virtual Machine Listing	Amazon Web Services listing of EC2 instances and properties	06/2021
AWS-06	AWS EC2 - Load Balancing	Amazon Web Services elastic load balancer listing and properties	06/2021
AWS-08	AWS CloudTrail Configuration & Logs	Amazon Web Services CloudTrail logging services and settings	06/2021

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
AWS-09	AWS CloudWatch Configuration & Logs	Amazon Web Services CloudWatch logging services and settings	07/2021
CHG-01	Change Records - Network Changes	Sample of ticket records for network changes that occurred	07/2021
CHG-02	Change Records - System Changes	Sample of ticket records for system changes & scheduled patches that occurred	08/2021
CHG-03	Change Records - Application Changes Deployed to Production	Sample of ticket records for application changes deployed into production	09/2021
CHG-05	Change Records - Significant Changes to Environment	Ticket records for significant changes to the environment	07/2021
CUS-01	Customer Contracts & Agreements	Customer contracts and agreements indicating the organization will maintain applicable PCI DSS requirements	09/2021
DB-01	Database User Listing & Access Permissions	Database user listing and permissions	06/2021
DB-03	Database Encryption Methods	Database encryption methods used to store sensitive information	06/2021
DB-04	Database Schema Listing	List of all available database schemas	06/2021
DEV-01	Code Repo & Versioning Tools - User Listing & Permissions	User listing and permissions for development tools such as code repositories / versioning and deployment tools	07/2021
DEV-02	Integration & Deployment Tools - User Listing & Permissions	Inventory of dev / test servers (include hostnames and IP addresses)	07/2021
DEV-04	Sanitization Between Test & Production Environments	Sanitization Between Test & Production Environments	08/2021
DGM-01	Network Diagrams	Network diagrams of the cardholder data environment	06/2021
DGM-02	Data Flow Diagrams	Data-flow diagrams of the services provided	06/2021
EMP-00	Employee Roster	Employee roster of personnel in scope of the assessment	08/2021
EMP-02.1	Employee Annual Security Awareness Refresher	Employee annual security awareness training completion	08/2021
EMP-03.1	Terminated Employee Access Removal Records	Terminated employee logical and physical access removal request records	12/2021

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
FIM-01	FIM - Monitored Files & Comparison Schedule	FIM software settings indicating objects to be monitored and schedule to compare changes	06/2021
IDS-01	IDS - Rule Sets & Signature Updates	IDS configuration settings for network interfaces and the rule sets enabled to inspect traffic flow for anomalous behavior	06/2021
LOG-01	Central Log System - User Listing & Permissions	Central log management user listing and permissions	06/2021
LOG-02	Central Log System - Log Retention	Central log management log retention period	06/2021
LOG-03	Central Log System - Log Settings & Examples	Central log management settings and example logs	06/2021
LOG-04	Central Log System - Alert Settings & Examples	Central log management alert settings and example alerts	07/2021
MED-01	Electronic Media Encryption & Restriction	Inventory and tracking documentation for employee-assigned secure token FOBs	08/2021
MED-03	Hard-copy Material Destruction	Certificate of Destruction or Chain of Custody document to evidence that the destruction of media was tracked and recorded	08/2021
MFA-01	MFA Login from Internal & External Networks	MFA login process to access the in-scope system components from both internal networks	06/2021
ORG-02	Job Descriptions	Job descriptions related to IT and security personnel responsible for the programs and systems in scope	07/2021
ORG-03	Employee Handbook & Code of Conduct	Employee Handbook that defines corporate ethic and code of conduct	07/2021
ORG-06	PCI DSS Compliance Program & Charter	Formal documentation and charter indicating that executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance	07/2021
PC-00	Inventory of PCs & Laptops in Scope	Inventory listing of laptops in scope	09/2021
PC-01	PC FW Settings - Actively Running & Prevent Disabling	PC settings indicating host-based firewall settings are enforced and can't be disabled	08/2021
PC-03.1	PC AV - Running & Prevent Disabling	PC settings indicating endpoint protection software are enforced and can't be disabled	08/2021
PC-03.2	PC AV - Update Schedule	PC settings indicating endpoint protection software are being updated with new virus definitions	08/2021

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
PC-03.3	PC AV - Scan Schedule	PC settings indicating endpoint protection software are enforced to scan at defined frequencies	08/2021
PC-03.4	PC AV - Detection Action	PC settings indicating endpoint protection software cleans or quarantines	08/2021
PC-04	PC Screen Saver Settings	VPN client configurations for PCs in scope	08/2021
PC-06	PC Hard Drive Encryption Settings	Hard drive encryption configurations for PCs in scope	08/2021
PHY-01	List of Users with Key & Badge Access to Sensitive Areas	Listing of users assigned keys and / or badges that provide access to sensitive areas	07/2021
PHY-02	Administrator Listing to Badge Access System	Listing of users with administrator permission to the badge access system	07/2021
POL-00	Dissemination of Policies & Procedures	Method used to disseminate the Information Security Policy	07/2021
POL-01	Data Security Policies and Procedures	Policies and procedures related to the implementation and maintenance of all PCI requirements to protect cardholder data	07/2021
PRV-00	Privacy Policy	Policies and procedures related to the implementation and maintenance of controls for restricting access to, retaining, and destroying protected information.	07/2021
RVW-01	Review of Firewall Rules	Evidence of semi-annual firewall review	07/2021
RVW-03.1	Review of Logical Access for Privileged Users	Evidence of quarterly access review of physical access (Badge access, assigned keys, etc.) for the Tampa scanning room.	07/2021
RVW-05	Review of Operational Procedures	Procedures and evidence of quarterly reviews to confirm personnel are following security policies and operational procedures	09/2021
RVW-06	Review Storage & Deletion of Protected Data Based on Retention	Evidence of the Tampa scanning room PCs showing Secure Erasure is used.	12/2021
SCN-01	Internal Vulnerability Scans	Evidence of quarterly internal vulnerability scans	08/2021
SCN-02	External Vulnerability Scans	Evidence of quarterly external ASV scans	08/2021
SCN-03	Significant Changes - Internal Vulnerability Scans	Internal vulnerability scans performed after significant changes	08/2021

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
SCN-04	Significant Changes - External Vulnerability Scans	External vulnerability scans performed after significant changes	08/2021
SP-00	Listing of Third-Party Service Providers	Listing of all service providers who can affect the security of cardholder data	08/2021
SP-01	Service Provider Contracts & Agreements	Third-party auditor reports for in-scope service providers indicating due diligence on service provider compliance to relevant PCI requirements	07/2021
SP-02	Service Provider Third-Party Auditor Reports	Third-party auditor reports for in-scope service providers indicating due diligence on service provider compliance to relevant PCI requirements	09/2021
SRV-00	Inventory of Servers in Scope	Inventory of all servers in scope	06/2021
SRV-01.0	Server Host & Network Information	Host and network information for in-scope servers	07/2021
SRV-01.1	Server User Listing & Access Permissions	User listing and permissions on in-scope servers	07/2021
SRV-01.2	Server Password & Account Lockout	Password and account lockout policies enforced for user accounts on in-scope servers	07/2021
SRV-01.3	Server Running Services & Listening Ports	Services and listening ports that are running on in-scope servers	07/2021
SRV-01.4	Server Installed Applications & Versions	Listing of installed applications on in-scope servers	07/2021
SRV-01.5	Server Patch Updates Installed & Settings	Listing of installed patches and updates on in-scope servers	07/2021
SRV-01.6	Server Remote Management & Idle Timeouts	Remote management configurations and timeout settings for inactive sessions on in-scope servers	07/2021
SRV-01.7	Server NTP Settings	NTP settings configured on in-scope servers	07/2021
SRV-01.8	Server Audit Settings & Local Log Examples	Audit log settings and example logs on in-scope servers	07/2021
SRV-02	Server Hardening Scripts & Security Enforcement	Configuration and hardening process used to secure deployed servers	07/2021
TRN-01	Security Awareness Training Material	Security awareness training material for new hire and annual training refreshers	07/2021
TRN-02	Developer Secure Coding Training	Secure coding training provided to development personnel	08/2021

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
VPN-01	VPN Client User Listing	VPN Client User Listing	06/2021
VPN-02	VPN Client Authentication & Encryption	VPN Client Authentication & Encryption	06/2021
WAF-01	WAF Configuration - Actively Running & Updated	Evidence that WAF software is running and up-to-date	07/2021
WAF-02	WAF Configuration - Block or Alert Rule Settings & Examples	Block and alert rule settings for WAF software in place	07/2021

4.10 Individuals interviewed

Identify and list the individuals interviewed. Include the following:

Reference Number *(optional)*	Employee Name	Role/Job Title	Organization	Is this person an ISA? (yes/no)
	Nadine Chahal	General Counsel	Fairfax	No
	Alex Umansky	Senior Software Engineer	Fairfax	No
	Robert Castello	Director of Support Services	Fairfax	No
	Maryanne Pearson	Controller	Fairfax	No

4.11 Managed service providers

For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans:

▪ Identify whether the entity being assessed is a managed service provider. **(yes/no)**	No
▪ *If "yes":*	
– List the requirements that apply to the MSP and are included in this assessment.	Not applicable
– List the requirements that are the responsibility of the MSP's customers (and have not been included in this assessment).	Not applicable
– Provide the name of the assessor who attests that the testing of these requirements and/or responsibilities of the MSP is accurately represented in the signed Attestation of Compliance.	Not applicable
– Identify which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans.	Not applicable
– Identify which of the MSP's IP addresses are the responsibility of the MSP's customers.	Not applicable

4.12 Disclosure summary for "In Place with Compensating Control" responses

▪ Identify whether there were any responses indicated as "In Place with Compensating Control." **(yes/no)**	No
▪ *If "yes," complete the table below:*	

List of all requirements/testing procedures with this result	**Summary of the issue** (legal obligation, etc.)
Not applicable	Not applicable

4.13 Disclosure summary for "Not Tested" responses

▪ Identify whether there were any responses indicated as "Not Tested": **(yes/no)**	No
▪ *If "yes," complete the table below:*	

List of all requirements/testing procedures with this result	**Summary of the issue** (for example, not deemed in scope for the assessment, etc.)
Not applicable	Not applicable

5. Quarterly Scan Results

5.1 Quarterly scan results

▪ Is this the assessed entity's initial PCI DSS compliance validation? **(yes/no)**	No

▪ Identify how many external quarterly ASV scans were performed within the last 12 months:	*4*

▪ *Summarize* the four most recent quarterly ASV scan results in the Summary Overview as well as in comments at Requirement 11.2.2.

Note: *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verified:*
- *The most recent scan result was a passing scan,*
- *The entity has documented policies and procedures requiring quarterly scanning going forward, and*
- *Any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan.*

For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.

▪ For each quarterly ASV scan performed within the last 12 months, identify:

Date of the scan(s)	Name of ASV that performed the scan	Were any vulnerabilities found that resulted in a failed initial scan? (yes/no)	For all scans resulting in a Fail, provide date(s) of re-scans showing that the vulnerabilities have been corrected
September 2, 2020	Aperia	No	No failing scans resulted.
December 2, 2020	Aperia	Yes	The findings were false positives and did not require a rescan. The ASV updated the scanning software to address these resulting in a clean scan during the next quarterly scan – March 3, 2021.
March 3, 2021	Aperia	No	No failing scans resulted.
June 2, 2021	Aperia	No	No failing scans resulted.

If this is the initial PCI DSS compliance validation*, complete the following:*	
▪ Provide the name of the assessor who attests that the most recent scan result was verified to be a passing scan.	Not Applicable. This is not Fairfax's initial PCI DCC compliance validation.
▪ Identify the name of the document the assessor verified to include the entity's documented policies and procedures requiring quarterly scanning going forward.	Not applicable.
▪ Describe how the assessor verified that any vulnerabilities noted in the initial scan have been corrected, as shown in a re-scan.	Not applicable.
Assessor comments, if applicable:	Not applicable.

5.2 Attestations of scan compliance

Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI DSS Approved Scanning Vendors (ASV) Program Guide.*

Provide the name of the assessor who attests that the ASV and the entity have completed the Attestations of Scan Compliance confirming that all externally accessible (Internet-facing) IP addresses in existence at the entity were appropriately scoped for the ASV scans:	Phillip Hagan, QSA # 203-736

6. Findings and Observations

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.			☒	☐	☐	☐	☐
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: ● Network connections, and ● Changes to firewall and router configurations.	**Identify the document(s)** reviewed to verify procedures define the formal processes for:						
	● Testing and approval of all network connections.	POL-01 Data Security Policies and Procedures					
	● Testing and approval of all changes to firewall and router configurations.	POL-01 Data Security Policies and Procedures					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	**Identify the sample of records** for network connections that were selected for this testing procedure.	CHG-01 Change Records - Network Changes					
	Identify the responsible personnel interviewed who confirm that network connections were approved and tested.	Alex Umansky - Senior Software Engineer					
	Describe how the sampled records verified that network connections were:						
	● Approved	360 Advanced inspected change request tickets to verify that processes included documentation of approval before changes were made. Personnel responsible for network management granted the approval for new network connections and changes to network configurations. Documentation Reviewed: CHG-01 Change Records - Network Changes					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Tested	360 Advanced inspected change request tickets to verify that processes included testing before case tickets were resolved and closed. Personnel responsible for network management tested new network connections and changes to network configurations. Documentation Reviewed: CHG-01 Change Records - Network Changes					
1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	**Identify the sample of records** for firewall and router configuration changes that were selected for this testing procedure.	CHG-01 Change Records - Network Changes					
	Identify the responsible personnel interviewed who confirm that changes made to firewall and router configurations were approved and tested.	Alex Umansky - Senior Software Engineer					
	Describe how the sampled records verified that the firewall and router configuration changes were:						
	• Approved	360 Advanced inspected change request tickets to verify that processes included documentation of approval before changes were made. Personnel responsible for network management granted the approval for new network connections and changes to network configurations. Documentation Reviewed: CHG-01 Change Records - Network Changes					
	• Tested	360 Advanced inspected change request tickets to verify that processes included testing before case tickets were resolved and closed. Personnel responsible for network management tested new network connections and changes to network configurations. Documentation Reviewed: CHG-01 Change Records - Network Changes					
1.1.2 Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.			☒	☐	☐	☐	☐
1.1.2.a Examine diagram(s) and observe network configurations to verify that a	**Identify the current network diagram**(s) examined.	DGM-01 Network Diagrams					
	Describe how network configurations verified that the diagram:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
current network diagram exists and that it documents all connections to the cardholder data environment, including any wireless networks.	• Is current.	360 Advanced inspected network diagrams and configurations to verify that network diagrams were consistent with the current network configurations in place. Documentation Reviewed: AWS-04 AWS VPC - Security Groups DGM-01 Network Diagrams DGM-02 Data Flow Diagrams SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					
	• Includes all connections to cardholder data.	360 Advanced inspected network diagrams and configurations to verify that network diagrams included all connections to the cardholder data environment. Documentation Reviewed: AWS-04 AWS VPC - Security Groups DGM-01 Network Diagrams DGM-02 Data Flow Diagrams SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					
	• Includes any wireless network connections.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	**Identify the responsible personnel** interviewed who confirm that the diagram is kept current.	Alex Umansky - Senior Software Engineer					
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.			☒	☐	☐	☐	☐
	Identify the data-flow diagram(s) examined.	DGM-02 Data Flow Diagrams					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1.3.a Examine data flow diagram and interview personnel to verify the diagram: ● Shows all cardholder data flows across systems and networks. ● Is kept current and updated as needed upon changes to the environment.	**Identify the responsible personnel** interviewed who confirm that the diagram: ● Shows all cardholder data flows across systems and networks. ● Is kept current and updated as needed upon changes to the environment.	Alex Umansky - Senior Software Engineer					
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.			☒	☐	☐	☐	☐
1.1.4.a Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	**Identify the firewall configuration standards document** examined to verify requirements for a firewall: ● At each Internet connection. ● Between any DMZ and the internal network zone.	POL-01 Data Security Policies and Procedures					
1.1.4.b Verify that the current network diagram is consistent with the firewall configuration standards.	**Provide the name of the assessor** who attests that the current network diagram is consistent with the firewall configuration standards.	Phillip Hagan, QSA# 204-876					
1.1.4.c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams.	**Describe how** network configurations verified that, per the documented configuration standards and network diagrams, a firewall is in place:						
	● At each Internet connection.	360 Advanced inspected AWS Inventory, security groups, and IP configurations to verify that a firewall is in place at each Internet connection. Network configurations indicated security zones between the Internet, DMZ, and private network segments. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Between any DMZ and the internal network zone.	360 Advanced inspected AWS inventory, security groups, and IP configurations to verify that a firewall is in place at each Internet connection. Network configurations indicated security zones between the Internet, DMZ, and private network segments. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					
1.1.5 Description of groups, roles, and responsibilities for management of network components.			☒	☐	☐	☐	☐
1.1.5.a Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.	**Identify the firewall and router configuration standards document(s)** reviewed to verify they include a description of groups, roles and responsibilities for management of network components.	POL-01 Data Security Policies and Procedures					
1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.	**Identify the responsible personnel** interviewed who confirm that roles and responsibilities are assigned as documented.	Nadine Chahal - General Counsel					
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.			☒	☐	☐	☐	☐
1.1.6.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each.	**Identify the firewall and router configuration standards document(s)** reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification and approval for each.	POL-01 Data Security Policies and Procedures					
1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.	**Indicate whether** any insecure services, protocols or ports are allowed. **(yes/no)**	Yes 1) HTTP TCP/80: Originating from internal network to be routed to the appropriate external server via the internet, and their responses permitted to enter. 2) HTTP TCP/80: Originating from the Internet, and their responses permitted to exit.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	If "yes," complete the instructions below for EACH insecure service, protocol, and port allowed: (add rows as needed)						
	Identify the firewall and router configuration standards document(s) reviewed to verify that security features are documented for each insecure service/protocol/port.	Documented justification is as follows: 1) Certain monitoring and update services require connections to be made over HTTP, and do not offer HTTPS alternatives. These applications are not transmitting cardholder data. 2) Users cannot make requests via HTTP, all requests come in via appropriate HTTPS URL Documentation Reviewed: POL-01 Data Security Policies and Procedures					
1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.	*If "yes" at 1.1.6.b, complete the following for each insecure service, protocol, and/or port present (add rows as needed):*						
	Describe how firewall and router configurations verified that the documented security features are implemented for each insecure service, protocol and/or port.	360 Advanced inspected AWS security groups and IP configurations to verify that the documented security features were implemented for each insecure service, protocol and/or port. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					
1.1.7 Requirement to review firewall and router rule sets at least every six months.			☒	☐	☐	☐	☐
1.1.7.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	**Identify the firewall and router configuration standards document(s)** reviewed to verify they require a review of firewall rule sets at least every six months.	POL-01 Data Security Policies and Procedures					
1.1.7.b Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.	**Identify the document(s) relating to rule set reviews** that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets.	RVW-01 Review of Firewall Rules					
	Identify the responsible personnel interviewed who confirm that rule sets are reviewed at least every six months for firewall and router rule sets.	Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*							
1.2 Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment:							
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.			☒	☐	☐	☐	☐
1.2.1.a Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.	**Identify the firewall and router configuration standards document(s)** reviewed to verify they identify inbound and outbound traffic necessary for the cardholder data environment.	POL-01 Data Security Policies and Procedures					
1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.	**Describe how** firewall and router configurations verified that the following traffic is limited to that which is necessary for the cardholder data environment:						
	• Inbound traffic	360 Advanced inspected AWS security groups and IP configurations and compared them with the documented services and firewall exceptions within the firewall policy. Inbound traffic was limited to IP addresses and protocols that were authorized as necessary for business purposes. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing AWS-06 AWS EC2 - Load Balancing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Outbound traffic	360 Advanced inspected AWS security groups and IP configurations and compared them with the documented services and firewall exceptions within the firewall policy. Outbound traffic was limited to IP addresses and protocols that were authorized as necessary for business purposes. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing AWS-06 AWS EC2 - Load Balancing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					
1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	**Describe how** firewall and router configurations verified that the following is specifically denied:						
	• All other inbound traffic	360 Advanced inspected AWS security groups and IP configurations and compared them with vendor documentation to verify that all other inbound traffic not explicitly allowed were either explicitly or implicitly denied. Review of vendor documentation verified that network devices employed a default "deny all" statement for inbound traffic on all interfaces. Documentation Reviewed: AWS-04 AWS VPC - Security Groups SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information Amazon EC2 Security Groups for Windows Instances: http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/concepts.html					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• All other outbound traffic	360 Advanced inspected AWS security groups and IP configurations and compared them with vendor documentation to verify that all other inbound traffic not explicitly allowed were either explicitly or implicitly denied. Review of vendor documentation verified that network devices employed a default "deny all" statement for outbound traffic on all interfaces. Documentation Reviewed: AWS-04 AWS VPC - Security Groups SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information Amazon EC2 Security Groups for Windows Instances: http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/concepts.html					
1.2.2 Secure and synchronize router configuration files.			☒	☐	☐	☐	☐
1.2.2.a Examine router configuration files to verify they are secured from unauthorized access.	**Describe how** router configuration files are secured from unauthorized access.	Routing and packet switching are handled by AWS objects that are not controlled by Fairfax. Security and synchronization of router configuration files are inherited by underlying infrastructure provided by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included testing procedures for this requirement within its own PCI assessment. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
1.2.2.b Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).	**Describe how** router configurations are synchronized.	Routing and packet switching are handled by AWS objects that are not controlled by Fairfax. Security and synchronization of router configuration files are inherited by underlying infrastructure provided by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included testing procedures for this requirement within its own PCI assessment. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.			☒	☐	☐	☐	☐
1.2.3.a Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.	**Describe how** firewall and router configurations verified that perimeter firewalls are in place between all wireless networks and the cardholder data environment.	360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
1.2.3.b Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**Indicate whether** traffic between the wireless environment and the cardholder data environment is necessary for business purposes. **(yes/no)**	360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	If "no":						
	Describe how firewall and/or router configurations verified that firewalls deny all traffic from any wireless environment into the cardholder environment.	360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	If "yes":						
	Describe how firewall and/or router configurations verified that firewalls permit only authorized traffic from any wireless environment into the cardholder environment.	360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.							
1.3 Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment:							
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.			☒	☐	☐	☐	☐
1.3.1 Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**Describe how** firewall and router configurations verified that the DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	360 Advanced inspected AWS security groups and IP configurations and compared them to the documented list of authorized services, protocols, and ports to verify that a DMZ was implemented to limit inbound traffic to only the system components specified. A separate DMZ segment was implemented that contained publicly accessible web services with firewall rule sets and NAT translations forwarding all authorized inbound traffic to specific IP addresses and ports within the DMZ network. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing AWS-06 AWS EC2 - Load Balancing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.			☒	☐	☐	☐	☐
1.3.2 Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.	**Describe how** firewall and router configurations verified that configurations limit inbound Internet traffic to IP addresses within the DMZ.	360 Advanced inspected AWS security groups and IP configurations and compared them to the documented list of authorized services, protocols, and ports to verify that a DMZ was implemented to limit inbound traffic to only the system components specified. A separate DMZ segment was implemented that contained publicly accessible web services with firewall rule sets and NAT translations forwarding all authorized inbound traffic to specific IP addresses and ports within the DMZ network. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing AWS-06 AWS EC2 - Load Balancing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. *(For example, block traffic originating from the Internet with an internal source address)*			☒	☐	☐	☐	☐
1.3.3 Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ**.**	**Describe how** firewall and router configurations verified that anti-spoofing measures are implemented.	360 Advanced inspected network configurations and compared them with vendor documentation to verify that anti-spoofing measures were in place to detect and block forged source IP addresses from entering the network. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-06 AWS EC2 - Load Balancing VPC Security Capabilities - https://aws.amazon.com/answers/networking/vpc-security-capabilities/					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.			☒	☐	☐	☐	☐
1.3.4 Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	**Describe how** firewall and router configurations verified that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	360 Advanced inspected AWS security groups and IP configurations and compared them to the documented list of authorized services, protocols, and ports to verify that outbound traffic from the CDE to the Internet was explicitly authorized as indicated in the documented exceptions. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-05 AWS EC2 - Virtual Machine Listing SRV-00 Inventory of Servers in Scope POL-01 Data Security Policies and Procedures					
1.3.5 Permit only "established" connections into the network.			☒	☐	☐	☐	☐
1.3.5 Examine firewall and router configurations to verify that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session.	**Describe how** firewall and router configurations verified that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session	360 Advanced inspected AWS security groups and IP configurations and compared them with vendor documentation to verify that security groups bound to AWS instances performed stateful packet inspection by default. Documentation Reviewed: AWS-04 AWS VPC - Security Groups SRV-00 Inventory of Servers in Scope Amazon EC2 Security Groups for Windows Instances: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html					
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.			☐	☐	☒	☐	☐
1.3.6 Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	**Indicate whether** any system components store cardholder data. **(yes/no)**	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					
	If "yes":						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how firewall and router configurations verified that the system components that store cardholder data are located on an internal network zone, and are segregated from the DMZ and other untrusted networks.	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. ● Note: Methods to obscure IP addressing may include, but are not limited to: ● Network Address Translation (NAT), ● Placing servers containing cardholder data behind proxy servers/firewalls, ● Removal or filtering of route advertisements for private networks that employ registered addressing, ● Internal use of RFC1918 address space instead of registered addresses.			☒	☐	☐	☐	☐
1.3.7.a Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	**Describe how** firewall and router configurations verified that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	360 Advanced inspected AWS security groups and IP configurations to verify that private IP addresses (RFC 1918) were used in conjunction with IP masquerading / NAT. In addition, the default configuration of disabling IP source routing within these components provides additional security to prevent disclosure of private IP addresses and routing information. Documentation Reviewed: AWS-03 AWS VPC - Virtual Networking AWS-04 AWS VPC - Security Groups AWS-06 AWS EC2 - Load Balancing SRV-00 Inventory of Servers in Scope SRV-01.0 Server Host & Network Information					
1.3.7.b Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.	**Identify the document** reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted.	POL-01 Data Security Policies and Procedures					
	For each permitted disclosure, **identify the responsible personnel** interviewed who confirm that the disclosure is authorized.	Nadine Chahal - General Counsel Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: ● Specific configuration settings are defined. ● Personal firewall (or equivalent functionality) is actively running. ● Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.			☒	☐	☐	☐	☐
1.4.a Examine policies and configuration standards to verify: ● Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. ● Specific configuration settings are defined for personal firewall or equivalent functionality. ● Personal firewall or equivalent functionality is configured to actively run. ● Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices.	**Indicate whether** portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network are used to access the organization's CDE. **(yes/no)**	Yes.					
	If "no," identify the document reviewed that explicitly prohibits portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network from being used to access the organization's CDE. ● *Mark 1.4.b as "not applicable"*	Not Applicable. Only a limited number of corporate-owned computers belonging to network and system administrators are configured to connect to the CDE via a secure VPN client connection using multi-factor network authentication.					
	If "yes," **identify the documented policies and configuration standards** that define the following: ● Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. ● Specific configuration settings are defined for personal firewall or equivalent functionality. ● Personal firewall or equivalent functionality is configured to actively run. ● Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices.	POL-01 Data Security Policies and Procedures					
	Identify the sample of mobile and/or employee-owned devices selected for this testing procedure.	Sample Set-2: Administrator Laptops					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.4.b Inspect a sample of portable computing devices (including company and/or employee-owned) to verify that: ● Personal firewall (or equivalent functionality) is installed and configured per the organization's specific configuration settings. ● Personal firewall (or equivalent functionality) is actively running. ● Personal firewall or equivalent functionality is not alterable by users of the portable computing devices.	**Describe how** the sample of portable computing devices (including company and/or employee-owned) verified that personal firewall software is:						
	● Installed and configured per the organization's specific configuration settings.	360 Advanced inspected laptop firewall configurations to verify that personal firewall software was configured per the organization's specific requirement settings. McAfee LiveSafe was used that enabled network protection through host-based inbound/outbound rules and application access protection. Documentation Reviewed: PC-01 PC FW Settings - Actively Running & Prevent Disabling					
	● Actively running.	360 Advanced inspected laptop firewall configurations and observed firewall service status to verify that personal firewall software was actively running. McAfee LiveSafe status was observed to be active and online. Documentation Reviewed: PC-01 PC FW Settings - Actively Running & Prevent Disabling					
	● Not alterable by users of mobile and/or employee-owned devices.	360 Advanced inspected laptop firewall configurations and observed personnel attempt to alter the personal firewall settings to verify that settings were not alterable by users. McAfee LiveSafe settings and service were greyed out and could not be disabled or stopped via Windows Group Policy enforcement. Documentation Reviewed: PC-01 PC FW Settings - Actively Running & Prevent Disabling					
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
1.5 Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are: ● Documented, ● In use, and ● Known to all affected parties.	**Identify the document reviewed** to verify that security policies and operational procedures for managing firewalls are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for managing firewalls are: ● In use ● Known to all affected parties	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.			☒	☐	☐	☐	☐
2.1.a Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	Identify the vendor manuals and sources on the Internet used to find vendor-supplied accounts/passwords.	Center for Internet Security - https://benchmarks.cisecurity.org CIS Microsoft Windows Server 2016 Benchmark CIS Microsoft Windows Server 2019 Benchmark CIS Microsoft SQL Server 2017 Benchmark CIS Benchmarks for Amazon Web Services Foundations NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html					
	For each item in the sample, **describe how** attempts to log on to the sample of devices and applications using default vendor-supplied accounts and passwords verified that all default passwords have been changed.	360 Advanced observed attempts to log on to the sampled devices with known default accounts and passwords to verify that these attempts failed indicating vendor-supplied defaults were changed.					
2.1.b For the sample of system components, verify that all unnecessary	*For each item in the sample of system components indicated at 2.1.a,* ***describe how*** *all unnecessary default accounts were verified to be* ***either****:*						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	• Removed	360 Advanced inspected the configurations on AWS instances. This included changing or removing vendor-supplied accounts and passwords (CIS Benchmark 10.2 Disable System Accounts) and disabling SNMP (CIS Benchmark 6.14 Ensure SNMP Server is not enabled). Documentation Reviewed: POL-01 Data Security Policies and Procedures Center for Internet Security - https://benchmarks.cisecurity.org CIS Microsoft Windows Server 2016 Benchmark CIS Microsoft Windows Server 2019 Benchmark CIS Microsoft SQL Server 2017 Benchmark CIS Benchmarks for Amazon Web Services Foundations NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html					
	• Disabled	360 Advanced inspected the configurations on AWS instances. This included changing or removing vendor-supplied accounts and passwords (CIS Benchmark 10.2 Disable System Accounts) and disabling SNMP (CIS Benchmark 6.14 Ensure SNMP Server is not enabled). Documentation Reviewed: POL-01 Data Security Policies and Procedures Center for Internet Security - https://benchmarks.cisecurity.org CIS Microsoft Windows Server 2016 Benchmark CIS Microsoft Windows Server 2019 Benchmark CIS Microsoft SQL Server 2017 Benchmark CIS Benchmarks for Amazon Web Services Foundations NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.1.c Interview personnel and examine supporting documentation to verify that: ● All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. ● Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	**Identify the responsible personnel** interviewed who verify that: ● All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. ● Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	Alex Umansky - Senior Software Engineer				
	Identify supporting documentation examined to verify that: ● All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. ● Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	POL-01 Data Security Policies and Procedures Center for Internet Security - https://benchmarks.cisecurity.org CIS Microsoft Windows Server 2016 Benchmark CIS Microsoft Windows Server 2019 Benchmark CIS Microsoft SQL Server 2017 Benchmark CIS Benchmarks for Amazon Web Services Foundations NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html					
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.			☐	☐	☒	☐	☐
2.1.1.a Interview responsible personnel and examine supporting documentation to verify that: ● Encryption keys were changed from default at installation	**Indicate whether** there are wireless environments connected to the cardholder data environment or transmitting cardholder data. **(yes/no)** ● *If "no," mark 2.1.1 as "Not Applicable" and proceed to 2.2.*	No.					
	If "yes":						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions.	**Identify the responsible personnel** interviewed who verify that encryption keys are changed: ● From default at installation ● Anytime anyone with knowledge of the keys leaves the company or changes positions.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	Identify supporting documentation examined to verify that: ● Encryption keys were changed from default at installation ● Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
2.1.1.b Interview personnel and examine policies and procedures to verify: ● Default SNMP community strings are required to be changed upon installation. ● Default passwords/phrases on access points are required to be changed upon installation.	**Identify the responsible personnel** interviewed who verify that: ● Default SNMP community strings are required to be changed upon installation. ● Default passwords/passphrases on access points are required to be changed upon installation.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	Identify policies and procedures examined to verify that: ● Default SNMP community strings are required to be changed upon installation. ● Default passwords/phrases on access points are required to be changed upon installation.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.1.1.c Examine vendor documentation and login to wireless devices, with system administrator help, to verify: ● Default SNMP community strings are not used. ● Default passwords/passphrases on access points are not used.	**Identify vendor documentation** examined to verify that: ● Default SNMP community strings are not used. ● Default passwords/passphrases on access points are not used.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	Describe how attempts to login to wireless devices verified that:						
	● Default SNMP community strings are not used.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	● Default passwords/passphrases on access points are not used.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
2.1.1.d Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for: ● Authentication over wireless networks ● Transmission over wireless networks	**Identify vendor documentation** examined to verify firmware on wireless devices is updated to support strong encryption for: ● Authentication over wireless networks ● Transmission over wireless networks	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how wireless configuration settings verified that firmware on wireless devices is updated to support strong encryption for:						
	• Authentication over wireless networks.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	• Transmission over wireless networks.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
2.1.1.e Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.	**Identify vendor documentation** examined to verify other security-related wireless vendor defaults were changed, if applicable.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	Describe how wireless configuration settings verified that other security-related wireless vendor defaults were changed, if applicable.	Not Applicable. 360 Advanced noted that Fairfax's CDE resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: ● Center for Internet Security (CIS) ● International Organization for Standardization (ISO) ● SysAdmin Audit Network Security (SANS) Institute ● National Institute of Standards Technology (NIST)			☒	☐	☐	☐	☐
2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	**Identify the documented system configuration standards** for all types of system components examined to verify the system configuration standards are consistent with industry-accepted hardening standards.	POL-01 Data Security Policies and Procedures					
	Provide the name of the assessor who attests that the system configuration standards are consistent with industry-accepted hardening standards.	Phillip Hagan, QSA# 204-876					
2.2.b Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.	**Identify the policy documentation** examined to verify that system configuration standards are updated as new vulnerability issues are identified.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that system configuration standards are updated as new vulnerability issues are identified.	Alex Umansky - Senior Software Engineer					
2.2.c Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.	**Identify the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.	Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.d Verify that system configuration standards include the following procedures for all types of system components: ● Changing of all vendor-supplied defaults and elimination of unnecessary default accounts ● Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server ● Enabling only necessary services, protocols, daemons, etc., as required for the function of the system ● Implementing additional security features for any required services, protocols or daemons that are considered to be insecure ● Configuring system security parameters to prevent misuse ● Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers	**Identify the system configuration standards** for all types of system components that include the following procedures: ● Changing of all vendor-supplied defaults and elimination of unnecessary default accounts ● Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server ● Enabling only necessary services, protocols, daemons, etc., as required for the function of the system ● Implementing additional security features for any required services, protocols or daemons that are considered to be insecure ● Configuring system security parameters to prevent misuse ● Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers	POL-01 Data Security Policies and Procedures				
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*			☒	☐	☐	☐	☐
2.2.1.a Select a sample of system components and inspect the system	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
configurations to verify that only one primary function is implemented per server.	*For each item in the sample*, **describe how** system configurations verified that only one primary function per server is implemented.	360 Advanced inspected a list of active services and open ports on each sampled component to verify that Fairfax implemented each system with only one primary function. Documentation Reviewed: SRV-01.3 Server Running Services & Listening Ports SRV-01.4 Server Installed Applications & Versions					
2.2.1.b If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device.	**Indicate whether** virtualization technologies are used. **(yes/no)**	Yes.					
	If "no," **describe how** systems were observed to verify that no virtualization technologies are used.	Not applicable.					
	If "yes":						
	Identify the sample of virtual system components or devices selected for this testing procedure.	Sample Set-1: Servers					
	For each virtual system component and device in the sample, **describe how** system configurations verified that only one primary function is implemented per virtual system component or device.	For each virtual device in the sample, 360 Advanced inspected a list of active services and open ports to verify that Fairfax implemented each system with only one primary function. Documentation Reviewed: SRV-01.3 Server Running Services & Listening Ports SRV-01.4 Server Installed Applications & Versions					
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.			☒	☐	☐	☐	☐
2.2.2.a Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	For each item in the sample, **describe how** the enabled system services, daemons, and protocols verified that only necessary services or protocols are enabled.	360 Advanced inspected a list of active services and open ports on the sampled systems to verify that only services, and protocols necessary for the primary server role were enabled. Documentation Reviewed: SRV-01.3 Server Running Services & Listening Ports SRV-01.4 Server Installed Applications & Versions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.2.b Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.	*For each item in the sample of system components from 2.2.2.a,* **indicate whether** any insecure services, daemons, or protocols are enabled. **(yes/no)** *If "no," mark the remainder of 2.2.2.b and 2.2.3 as "Not Applicable."*	No.					
	If "yes," **identify the responsible personnel** interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol	Alex Umansky - Senior Software Engineer					
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure			☐	☐	☒	☐	☐
2.2.3 Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols.	*If "yes" at 2.2.2.b, perform the following:*						
	Describe how configuration settings verified that security features for all insecure services, daemons, or protocols are:						
	• Documented	Not Applicable. Insecure services, daemons, or protocols are not enabled.					
	• Implemented	Not Applicable. Insecure services, daemons, or protocols are not enabled.					
2.2.4 Configure system security parameters to prevent misuse.			☒	☐	☐	☐	☐
2.2.4.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.	**Identify the system administrators and/or security managers** interviewed for this testing procedure.	Alex Umansky - Senior Software Engineer					
	For the interview, **summarize the relevant details** discussed to verify that they have knowledge of common security parameter settings for system components.	360 Advanced inquired of responsible personnel to verify that they had knowledge of common security parameter settings for the system components in scope. The CIS AWS and Windows Server Benchmark were discussed and reviewed and verified that common security parameters for server hardening were included and properly identified within the document. Personnel also demonstrated familiarity with AWS security parameters such as security groups, network ACLs, availability zones, and access control settings within the IAM interface.					
2.2.4.b Examine the system configuration standards to verify that common security parameter settings are included.	**Identify the system configuration standards** examined to verify that common security parameter settings are included.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.4.c Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.	**Identify the sample** of system components selected for this testing procedure.	360 Advanced inspected security parameters and compared them to the System Component Configuration Standard. All provisioned instances are built to these standards. This process is incorporated into Fairfax's infrastructure build pipeline. Documentation Reviewed: POL-01 Data Security Policies and Procedures SRV-02 Server Hardening Scripts & Security Enforcement					
	For each item in the sample, **describe how** the common security parameters verified that they are set appropriately and in accordance with the configuration standards.	360 Advanced inspected security parameters and compared them to the System Component Configuration Standard. All provisioned instances are built to these standards. This process is incorporated into Fairfax's infrastructure build pipeline. Documentation Reviewed: POL-01 Data Security Policies and Procedures SRV-02 Server Hardening Scripts & Security Enforcement					
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.			☒	☐	☐	☐	☐
2.2.5.a Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	For each item in the sample, **describe how** configurations verified that all unnecessary functionality is removed.	360 Advanced inspected a list of active services on the sampled systems and identified only services, and protocols necessary for the server role, with no unnecessary functionality present. Documentation Reviewed: SRV-01.3 Server Running Services & Listening Ports SRV-01.4 Server Installed Applications & Versions					
2.2.5.b. Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration.	**Describe how** the security parameters and relevant documentation verified that enabled functions are:						
	• Documented	360 Advanced inspected policy sections pertaining to configuration standards and compared those settings with system security parameters to verify that specific standards for configuration and system hardening for enabled functions were documented. Documentation Reviewed: POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Support secure configuration	360 Advanced inspected system configurations on the sampled systems to verify that system standards were developed with parameters that supported secure configuration. Documentation Reviewed: SRV-02 Server Hardening Scripts & Security Enforcement					
2.2.5.c. Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components.	**Identify documentation** examined for this testing procedure.	POL-01 Data Security Policies and Procedures					
	Describe how the security parameters verified that only documented functionality is present on the sampled system components from 2.2.5.a.	360 Advanced inspected system configurations on the sampled systems and compared them with Fairfax documentation to verify that only documented services, and protocols appropriate for each server role were documented. Documentation Reviewed: POL-01 Data Security Policies and Procedures SRV-02 Server Hardening Scripts & Security Enforcement					
2.3 Encrypt all non-console administrative access using strong cryptography.			☒	☐	☐	☐	☐
2.3 Select a sample of system components and verify that non-console administrative access is encrypted by performing the following:	**Identify the sample** of system components selected for 2.3.a-2.3.d.	Sample Set-1: Servers					
2.3.a Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.	*For each item in the sample from 2.3:*						
	Describe how the administrator log on to each system verified that a strong encryption method is invoked before the administrator's password is requested.	360 Advanced observed non-console administrative log on to verify that a strong encryption method was invoked before the administrator's password was requested. Administrators first established an SSL VPN client session using two-factor authentication. An encrypted RDP session was then established through the VPN connection to gain non-console administrative access to system components. 360 Advanced noted that Amazon AWS management console access was established through a secured HTTPS session with MFA enabled for all user accounts. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA MFA-01 MFA Login from Internal & External Networks SRV-01.3 Server Running Services & Listening Ports VPN-02 VPN Client Authentication & Encryption					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how system configurations for each system verified that a strong encryption method is invoked before the administrator's password is requested.	360 Advanced inspected network and system configurations to verify that strong encryption was in use for non-console administrative access. Remote login services running indicated protocols in use that supported strong encryption. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA MFA-01 MFA Login from Internal & External Networks SRV-01.3 Server Running Services & Listening Ports VPN-02 VPN Client Authentication & Encryption					
	Identify the strong encryption method used for non-console administrative access.	RDP - High Encryption HTTPS - TLS 1.2 SSL VPN - TLS 1.2 NOTE: RDP sessions are established to assigned jump servers after connecting to the Amazon AWS environment via an SSL VPN client using multi-factor authentication.					
2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.	*For each item in the sample from 2.3:*						
	Describe how services and parameter files on systems verified that Telnet and other insecure remote-login commands are not available for non-console access.	360 Advanced inspected a list of active services on the sampled system components to verify that Telnet or other insecure remote login protocols were not enabled. Additionally, penetration testing results detected no instances of Telnet or other insecure remote login services were available for non-console access. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation SRV-01.3 Server Running Services & Listening Ports					
2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.	*For each item in the sample from 2.3:*						
	Describe how the administrator log on to each system verified that administrator access to any web-based management interfaces was encrypted with strong cryptography.	360 Advanced observed administrators accessing web-based management interfaces and noted that all instances utilized HTTPS. Additionally, the annual penetration testing detected no instances of web-based management interfaces lacking strong cryptography.					
	Identify the strong encryption method used for any web-based management interfaces.	HTTPS (TLS v1.2) with AES 256-bit					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.3.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	**Identify the vendor documentation** examined to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	Center for Internet Security - https://benchmarks.cisecurity.org CIS Microsoft Windows Server 2016 Benchmark CIS Microsoft Windows Server 2019 Benchmark CIS Microsoft SQL Server 2017 Benchmark CIS Benchmarks for Amazon Web Services Foundations					
	Identify the responsible personnel interviewed who confirm that that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	Alex Umansky - Senior Software Engineer					
2.4 Maintain an inventory of system components that are in scope for PCI DSS.			☒	☐	☐	☐	☐
2.4.a Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.	**Describe how** the system inventory verified that a list of hardware and software components is:						
	• Maintained	360 Advanced inspected an inventory document to verify that a list of virtual servers and software components were maintained. The items included in the inventory matched the network diagram and system components and software observed during the assessment. Documentation Reviewed: SRV-00 Inventory of Servers in Scope PC-00 Inventory of PCs & Laptops in Scope					
	• Includes a description of function/use for each	360 Advanced inspected the inventory document to verify that a list of virtual servers and software components included a description of function/use for each. The items included a description column describing the usage scenario for each component. Documentation Reviewed: SRV-00 Inventory of Servers in Scope PC-00 Inventory of PCs & Laptops in Scope					
2.4.b Interview personnel to verify the documented inventory is kept current.	**Identify the responsible personnel** interviewed who confirm that the documented inventory is kept current.	Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
2.5 Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are: ● Documented, ● In use, and ● Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for managing vendor defaults and other security parameters are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for managing vendor defaults and other security parameters are: ● In use ● Known to all affected parties	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.*			☐	☐	☒	☐	☐
2.6 Perform testing procedures **A1.1** through **A1.4** detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.	**Indicate whether** the assessed entity is a shared hosting provider. **(yes/no)**	No.					
	If "yes," **provide the name of the assessor** who attests that Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers has been completed.	Not Applicable. 360 Advanced verified that Fairfax is not serving as a shared hosting provider to their customers.					

Protect Stored Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.1 Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage: ● Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. ● Specific retention requirements for cardholder data ● Processes for secure deletion of data when no longer needed. ● A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.			☒	☐	☐	☐	☐
3.1.a Examine the data-retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage: ● Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. ● Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). ● Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons ● A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	**Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all cardholder data (CHD) storage: ● Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. ● Specific requirements for retention of cardholder data. ● Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. ● A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	POL-01 Data Security Policies and Procedures				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.1.b Interview personnel to verify that: ● All locations of stored cardholder data are included in the data-retention and disposal processes. ● Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. ● The quarterly automatic or manual process is performed for all locations of cardholder data.	**Identify the responsible personnel** interviewed who confirm that: ● All locations of stored cardholder data are included in the data-retention and disposal processes. ● Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. ● The quarterly automatic or manual process is performed for all locations of cardholder data.	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
3.1.c For a sample of system components that store cardholder data: ● Examine files and system records to verify that the data stored does not exceed the requirements defined in the data-retention policy. ● Observe the deletion mechanism to verify data is deleted securely.	**Identify the sample** of system components selected for this testing procedure.	Data Processing Workstations: INBVAE9 (RP2) DESKTOP-31S1S2M (RP4)					
	For each item in the sample, **describe how** files and system records verified that the data stored does not exceed the requirements defined in the data-retention policy.	360 Advanced inspected secure deletion software executed on batch archive folder to verify that processes were in place to purge cardholder data that exceeded the requirements defined in the data-retention policy. The software securely deleted files containing fields associated with cardholder data. Documentation Reviewed: RVW-06 Review Storage & Deletion of Protected Data Based on Retention					
	Describe how the deletion mechanism was observed to verify data is deleted securely.	360 Advanced inspected secure deletion software executed on batch archive folder to verify that deletion mechanisms were in place to securely delete files containing fields associated with cardholder data. The software was configured to overwrite data at least seven times using German BSI-VSITR or US DoD 5220.22-M ECE standards. Documentation Reviewed: RVW-06 Review Storage & Deletion of Protected Data Based on Retention					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* ● *There is a business justification, and* ● *The data is stored securely.* ● *Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:*			☐	☐	☒	☐	☐
3.2.a For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.	**Indicate whether** the assessed entity is an issuer or supports issuing service. **(yes/no)**	Not Applicable. Fairfax is neither an issuer nor does not offer issuing support services. In addition, Fairfax does not store sensitive authentication data such as card validation codes / values, full track data, PINs, and PIN blocks.					
	If "yes," complete the responses for 3.2.a and 3.2.b and mark 3.2.c and 3.2.d as "Not Applicable." *If "no," mark the remainder of 3.2.a and 3.2.b as "Not Applicable" and proceed to 3.2.c and 3.2.d.*						
	Identify the documentation reviewed to verify there is a documented business justification for the storage of sensitive authentication data.	Not Applicable. Fairfax is neither an issuer nor does not offer issuing support services. In addition, Fairfax does not store sensitive authentication data such as card validation codes / values, full track data, PINs, and PIN blocks.					
	Identify the interviewed personnel who confirm there is a documented business justification for the storage of sensitive authentication data.	Not Applicable. Fairfax is neither an issuer nor does not offer issuing support services. In addition, Fairfax does not store sensitive authentication data such as card validation codes / values, full track data, PINs, and PIN blocks.					
	For the interview, **summarize the relevant details** of the business justification described.	Not Applicable. Fairfax is neither an issuer nor does not offer issuing support services. In addition, Fairfax does not store sensitive authentication data such as card validation codes / values, full track data, PINs, and PIN blocks.					
3.2.b For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured.	*If "yes" at 3.2.a,*						
	Identify data stores examined.	Not Applicable. Fairfax is neither an issuer nor does not offer issuing support services. In addition, Fairfax does not store sensitive authentication data such as card validation codes / values, full track data, PINs, and PIN blocks.					
	Describe how the data stores and system configurations were examined to verify that the sensitive authentication data is secured.	Not Applicable. Fairfax is neither an issuer nor does not offer issuing support services. In addition, Fairfax does not store sensitive authentication data such as card validation codes / values, full track data, PINs, and PIN blocks.					
3.2.c For all other entities, if sensitive authentication data is received, review policies and procedures, and examine	**Indicate whether** sensitive authentication data is received. **(yes/no)**	No.					
	If "yes," complete 3.2.c and 3.2.d. *If "no," mark the remainder of 3.2.c and 3.2.d as "Not Applicable" and proceed to 3.2.1.*						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
system configurations to verify the data is not retained after authorization.	**Identify the document(s)** reviewed to verify the data is not retained after authorization.	Not Applicable. Fairfax does not receive sensitive authentication data.					
	Describe how system configurations verified that the data is not retained after authorization.	Not Applicable. Fairfax does not receive sensitive authentication data.					
3.2.d For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable.	**Identify the document(s)** reviewed to verify that it defines processes for securely deleting the data so that it is unrecoverable.	Not Applicable. Fairfax does not receive sensitive authentication data.					
	Describe how the processes for securely deleting the data were examined to verify that the data is unrecoverable.	Not Applicable. Fairfax does not receive sensitive authentication data.					
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ● *The cardholder's name* ● *Primary account number (PAN)* ● *Expiration date* ● *Service code* *To minimize risk, store only these data elements as needed for business.*			☒	☐		☐	☐
3.2.1 For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization: ● Incoming transaction data ● All logs (for example, transaction, history, debugging, error) ● History files ● Trace files ● Several database schemas	**Identify the sample** of system components selected for 3.2.1-3.2.3.	Sample Set-1: Servers					
	For each data source type below from the sample of system of components examined, **summarize the specific examples of each data source type observed** to verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization. If that type of data source is not present, indicate that in the space.						
	● Incoming transaction data	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	● All logs (for example, transaction, history, debugging error)	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Database contents	• History files	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Trace files	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Database schemas	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Database contents	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• If applicable, any other output observed to be generated	Not Applicable.					
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization.			☒	☐		☐	☐
3.2.2 For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files	*For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. If that type of data source is not present, indicate that in the space.						
	• Incoming transaction data	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• All logs (for example, transaction, history, debugging error)	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Trace files • Several database schemas • Database contents	• History files	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Trace files	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Database schemas	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Database contents	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• If applicable, any other output observed to be generated	Not Applicable.					
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.			☒	☐		☐	☐
3.2.3 For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents	*For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed**. If that type of data source is not present, indicate that in the space.						
	• Incoming transaction data	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• All logs (for example, transaction, history, debugging error)	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• History files	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Trace files	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Database schemas	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• Database contents	The Quick Modules workflow involves the receipt of only CHD on paper form. SAD is not included within the paper form and therefore cannot be extracted or deduced in any way to be stored within logs, databases, or any other form of output.					
	• If applicable, any other output observed to be generated	Not Applicable.					
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN. ***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*			☒	☐	☐	☐	☐
3.3.a Examine written policies and procedures for masking the display of PANs to verify: • A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	**Identify the document(s)** reviewed to verify that written policies and procedures for masking the displays of PANs include the following: • A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	POL-01 Data Security Policies and Procedures				
	Describe how system configurations verified that:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.3.b Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests.	• Full PAN is only displayed for users/roles with a documented business need.	The Quick Modules workflow involves the receipt of CHD on paper form which is restricted to data processing personnel who scan the form into a designated workstation which sends the image to the AWS environment. The CHD field is then extracted via the OCR engine and stored within a database residing on an encrypted EBS volume. The images and CHD stored on the database are restricted only to the Engineering team. There are no frontend interfaces that displays full or masked PANs.					
	• PAN is masked for all other requests.	The Quick Modules workflow involves the receipt of CHD on paper form which is restricted to data processing personnel who scan the form into a designated workstation which sends the image to the AWS environment. The CHD field is then extracted via the OCR engine and stored within a database residing on an encrypted EBS volume. The images and CHD stored on the database are restricted only to the Engineering team. There are no frontend interfaces that displays full or masked PANs.					
3.3.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see more than first six/last four digits of the PAN.	**Describe how** displays of PAN verified that:						
	• PANs are masked when displaying cardholder data.	The Quick Modules workflow involves the receipt of CHD on paper form which is restricted to data processing personnel who scan the form into a designated workstation which sends the image to the AWS environment. The CHD field is then extracted via the OCR engine and stored within a database residing on an encrypted EBS volume. The images and CHD stored on the database are restricted only to the Engineering team. There are no frontend interfaces that displays full or masked PANs.					
	• Only those with a legitimate business need are able to see more than first six/last four digits of the PAN.	The Quick Modules workflow involves the receipt of CHD on paper form which is restricted to data processing personnel who scan the form into a designated workstation which sends the image to the AWS environment. The CHD field is then extracted via the OCR engine and stored within a database residing on an encrypted EBS volume. The images and CHD stored on the database are restricted only to the Engineering team. There are no frontend interfaces that displays full or masked PANs.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ● One-way hashes based on strong cryptography, (hash must be of the entire PAN). ● Truncation (hashing cannot be used to replace the truncated segment of PAN). ● Index tokens and pads (pads must be securely stored). ● Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*			☒	☐	☐	☐	☐
3.4.a Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: ● One-way hashes based on strong cryptography ● Truncation ● Index tokens and pads, with the pads being securely stored ● Strong cryptography, with associated key-management processes and procedures	**Identify the documentation** examined to verify that the PAN is rendered unreadable using any of the following methods: ● One-way hashes based on strong cryptography, ● Truncation ● Index tokens and pads, with the pads being securely stored ● Strong cryptography, with associated key-management processes and procedures	POL-01 Data Security Policies and Procedures					
3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).	**Identify the sample** of data repositories selected for this testing procedure.	Amazon EBS Volumes					
	Identify the tables or files examined for each item in the sample of data repositories.	Amazon EBS Volume Name: NJTP DB1 D					
	For each item in the sample, **describe how** the tables or files verified that the PAN is rendered unreadable.	360 Advanced inspected EBS volume settings to verify that PAN was rendered unreadable. The database storing scanned images and extracted CHD resided in an EBS volume encrypted using AWS-managed keys.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.4.c Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable.	**Identify the sample** of removable media selected for this testing procedure.	Not Applicable. Fairfax does not store or backup cardholder data onto removable media.					
	For each item in the sample, **describe how** the sample of removable media confirmed that the PAN is rendered unreadable.	Not Applicable. Fairfax does not store or backup cardholder data onto removable media.					
3.4.d Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs.	**Identify the sample** of audit logs, including payment application logs, selected for this testing procedure.	Database logs Server event logs					
	For each item in the sample, **describe how** the sample of audit logs, including payment application logs, confirmed that the PAN is rendered unreadable or is not present in the logs.	360 Advanced inspected audit logs from the sample of system components to verify that PANs were not stored within the audit logs. The logs viewed did not contain any CHD including PANs. In addition, all data is rendered unreadable with AES 256-bit encryption using encrypted EBS volumes. Documentation Reviewed: DB-03 Database Encryption Methods LOG-03 Central Log System - Log Settings & Examples					
3.4.e If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	**Identify whether** hashed and truncated versions of the same PAN are present in the environment **(yes/no)** *If 'no,'* mark 3.4.e as 'not applicable' and proceed to 3.4.1.	No.					
	If 'yes,' **describe** the implemented controls examined to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	Not Applicable. Fairfax did not store hashed and truncated versions of the same PAN within their environment.					
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. ***Note:*** *This requirement applies in addition to all other PCI DSS encryption and key management requirements.*			☒	☐	☐	☐	☐
3.4.1.a If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is	**Indicate whether** disk encryption is used. **(yes/no)**	Yes.					
	If "yes," complete the remainder of 3.4.1.a, 3.4.1.b, and 3.4.1.c. *If "no," mark the remainder of 3.4.1.a, 3.4.1.b and 3.4.1.c as "Not Applicable."*						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials).	**Describe** the disk encryption mechanism(s) in use.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS. For the workstations located within the secure data processing room at the Tampa facility, BitLocker is enabled with keys uniquely generated outside of user accounts using each workstation's onboard Trusted Platform Module (TPM) chip. Documentation Reviewed: PC-06 PC Hard Drive Encryption Settings					
	For each disk encryption mechanism in use, **describe how** the configuration verified that logical access to encrypted file systems is separate from the native operating system's authentication mechanism.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS. For the workstations located within the secure data processing room at the Tampa facility, BitLocker is enabled with keys uniquely generated outside of user accounts using each workstation's onboard Trusted Platform Module (TPM) chip. Documentation Reviewed: PC-06 PC Hard Drive Encryption Settings					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	For each disk encryption mechanism in use, **describe how** the authentication process was observed to verify that logical access to encrypted file systems is separate from the native operating system's authentication mechanism.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS. For the workstations located within the secure data processing room at the Tampa facility, BitLocker is enabled with keys uniquely generated outside of user accounts using each workstation's onboard Trusted Platform Module (TPM) chip. Documentation Reviewed: PC-06 PC Hard Drive Encryption Settings					
3.4.1.b Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	**Describe how** processes were observed to verify that cryptographic keys are stored securely.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS. For the workstations located within the secure data processing room at the Tampa facility, BitLocker is enabled with keys uniquely generated outside of user accounts using each workstation's onboard Trusted Platform Module (TPM) chip. Documentation Reviewed: PC-06 PC Hard Drive Encryption Settings					
	Identify the responsible personnel interviewed who confirm that cryptographic keys are stored securely.	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
3.4.1.c Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored. ***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*	**Describe how** the configurations verified that cardholder data on removable media is encrypted wherever stored.	Not Applicable. Fairfax does not store or backup cardholder data onto removable media.					
	Describe how processes were observed to verify that cardholder data on removable media is encrypted wherever stored.	Not Applicable. Fairfax does not store or backup cardholder data onto removable media.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*			☒	☐	☐	☐	☐
3.5 Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: ● Access to keys is restricted to the fewest number of custodians necessary. ● Key-encrypting keys are at least as strong as the data-encrypting keys they protect. ● Key-encrypting keys are stored separately from data-encrypting keys. ● Keys are stored securely in the fewest possible locations and forms.	**Identify the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: ● Access to keys is restricted to the fewest number of custodians necessary. ● Key-encrypting keys are at least as strong as the data-encrypting keys they protect. ● Key-encrypting keys are stored separately from data-encrypting keys. ● Keys are stored securely in the fewest possible locations and forms.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.5.1 ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes: ● Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date ● Description of the key usage for each key. ● Inventory of any HSMs and other SCDs used for key management			☒	☐	☐	☐	☐
3.5.1 Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including: ● Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date	**Identify the responsible personnel interviewed** who confirm that a document exists to describe the cryptographic architecture, including: ● Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date ● Description of the key usage for each key ● Inventory of any HSMs and other SCDs used for key management	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● Description of the key usage for each key ● Inventory of any HSMs and other SCDs used for key management	**Identify the documentation reviewed** to verify that it contains a description of the cryptographic architecture, including: ● Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date ● Description of the key usage for each key ● Inventory of any HSMs and other SCDs used for key management	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.			☒	☐	☐	☐	☐
3.5.2 Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	**Identify user access lists** examined.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
	Describe how the user access lists verified that access to keys is restricted to the fewest number of custodians necessary.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: ● Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. ● Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). ● As at least two full-length key components or key shares, in accordance with an industry-accepted method. ***Note:*** *It is not required that public keys be stored in one of these forms.*			☒	☐	☐	☐	☐
3.5.3.a Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. ● Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. ● Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). ● As key components or key shares, in accordance with an industry-accepted method.	**Identify the documented procedures** examined to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. ● Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. ● Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). ● As key components or key shares, in accordance with an industry-accepted method.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.5.3.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one, (or more), of the following form at all times.	**Provide the name of the assessor** who attests that all locations where keys are stored were identified.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● Encrypted with a key-encrypting key. ● Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). ● As key components or key shares, in accordance with an industry-accepted method.	**Describe how** system configurations and key storage locations verified that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. ● Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. ● Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). ● As key components or key shares, in accordance with an industry-accepted method.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.5.3.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: ● Key-encrypting keys are at least as strong as the data-encrypting keys they protect. ● Key-encrypting keys are stored separately from data-encrypting keys.	**Describe how** system configurations and key storage locations verified that, wherever key-encrypting keys are used:						
	● Key-encrypting keys are at least as strong as the data-encrypting keys they protect	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
	● Key-encrypting keys are stored separately from data-encrypting keys.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.5.4 Store cryptographic keys in the fewest possible locations.			☒	☐	☐	☐	☐
3.5.4 Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	**Describe how** key storage locations and the observed processes verified that keys are stored in the fewest possible locations.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*			☐	☐	☒	☐	☐
3.6.a ***Additional Procedure for service provider assessments only***: If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers' keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	**Indicate whether** the assessed entity is a service provider that shares keys with their customers for transmission or storage of cardholder data. **(yes/no)**	No.					
	If "yes," **Identify the document** that the service provider provides to their customers examined to verify that it includes guidance on how to securely transmit, store and update customers' keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	Not Applicable. Fairfax does not share encryption keys with its customers or entities outside of the organization.					
3.6.b Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following:							
3.6.1 Generation of strong cryptographic keys.			☒	☐	☐	☐	☐
3.6.1.a Verify that key-management procedures specify how to generate strong keys.	**Identify the documented key-management procedures** examined to verify procedures specify how to generate strong keys.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.6.1.b Observe the procedures for generating keys to verify that strong keys are generated.	**Describe how** the procedures for generating keys was observed to verify that strong keys are generated.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.2 Secure cryptographic key distribution.			☒	☐	☐	☐	☐
3.6.2.a Verify that key-management procedures specify how to securely distribute keys.	**Identify the documented key-management procedures** examined to verify procedures specify how to securely distribute keys.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.6.2.b Observe the method for distributing keys to verify that keys are distributed securely.	**Describe how** the method for distributing keys was observed to verify that keys are distributed securely.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.6.3 Secure cryptographic key storage.			☒	☐	☐	☐	☐
3.6.3.a Verify that key-management procedures specify how to securely store keys.	**Identify the documented key-management procedures** examined to verify procedures specify how to securely store keys.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					
3.6.3.b Observe the method for storing keys to verify that keys are stored securely.	**Describe how** the method for storing keys was observed to verify that keys are stored securely.	360 Advanced confirmed that the Quick Modules infrastructure leverages encryption provided through AWS Key Management Service (KMS). Volumes containing the database that would store scanned images and extracted CHD were encrypted using AWS-managed encryption keys. The encryption process including key generation, key distribution, and key storage is outside the management of Fairfax and is fully managed by AWS.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).			☒	☐	☐	☐	☐
3.6.4.a Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s).	**Identify the documented key-management procedures** examined to verify procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s).	POL-01 Data Security Policies and Procedures					
3.6.4.b Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s).	**Identify** the responsible **personnel interviewed** who confirm that keys are changed at the end of the defined cryptoperiod(s).	Alex Umansky - Senior Software Engineer					
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*			☒	☐	☐	☐	☐
3.6.5.a Verify that key-management procedures specify processes for the following: ● The retirement or replacement of keys when the integrity of the key has been weakened. ● The replacement of known or suspected compromised keys. ● Any keys retained after retiring or replacing are not used for encryption operations.	**Identify the documented key-management procedures** examined to verify that key-management processes specify the following: ● The retirement or replacement of keys when the integrity of the key has been weakened. ● The replacement of known or suspected compromised keys. ● Any keys retained after retiring or replacing are not used for encryption operations.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.5.b Interview personnel to verify the following processes are implemented: ● Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. ● Keys are replaced if known or suspected to be compromised. ● Any keys retained after retiring or replacing are not used for encryption operations.	**Identify the responsible personnel** interviewed who confirm that the following processes are implemented: ● Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. ● Keys are replaced if known or suspected to be compromised. ● Any keys retained after retiring or replacing are not used for encryption operations.	Alex Umansky - Senior Software Engineer					
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. ***Note:*** *Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*			☐	☐	☒	☐	☐
3.6.6.a Verify that manual clear-text key-management procedures specify processes for the use of the following: ● Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND ● Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another.	**Indicate whether** manual clear-text cryptographic key-management operations are used. **(yes/no)**	No.					
	If "no," mark the remainder of 3.6.6.a and 3.6.6.b as "Not Applicable." *f "yes," complete 3.6.6.a and 3.6.6.b.*						
	Identify the documented key-management procedures examined to verify that manual clear-text key-management procedures define processes for the use of the following: ● Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND ● Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials of another.	Not Applicable. Fairfax does not perform manual clear-text cryptographic key-management operations.					
	Identify the responsible personnel interviewed for this testing procedure, if applicable.	Not Applicable. Fairfax does not perform manual clear-text cryptographic key-management operations.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.6 b Interview personnel and/or observe processes to verify that manual clear-text keys are managed with: ● Split knowledge, AND ● Dual control	For the interview, **summarize the relevant details discussed and/or describe how** processes were observed to verify that manual clear-text keys are managed with:						
	● Split knowledge	Not Applicable. Fairfax does not perform manual clear-text cryptographic key-management operations.					
	● Dual Control	Not Applicable. Fairfax does not perform manual clear-text cryptographic key-management operations.					
3.6.7 Prevention of unauthorized substitution of cryptographic keys.			☒	☐	☐	☐	☐
3.6.7.a Verify that key-management procedures specify processes to prevent unauthorized substitution of keys.	**Identify the documented key-management procedures** examined to verify that key-management procedures specify processes to prevent unauthorized substitution of keys.	POL-01 Data Security Policies and Procedures					
3.6.7.b Interview personnel and/or observe process to verify that unauthorized substitution of keys is prevented.	**Identify the responsible personnel** interviewed for this testing procedure, if applicable.	Alex Umansky - Senior Software Engineer					
	For the interview, **summarize the relevant details discussed and/or describe how** processes were observed to verify that unauthorized substitution of keys is prevented.	360 Advanced noted that encryption keys+L320:L336 used by an Amazon EBS volume can't be changed. However, a snapshot of the volume can be used to create a new, encrypted copy of the volume. While creating the new volume, a new encryption key can be specified. This process can only be performed through the AWS Management Console which was restricted to the Engineering team.					
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.			☒	☐	☐	☐	☐
3.6.8.a Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**Identify the documented key-management procedures** examined to verify that key-management procedures specify processes for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.8.b Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**Describe how** key custodian acknowledgements or other evidence were observed to verify that key custodians have acknowledged that they understand and accept their key-custodian responsibilities.	360 Advanced inspected signed policy acknowledgements to verify that written documents were maintained where personnel acknowledged that they understood and accepted their responsibilities to maintain security of CHD as specified within those policies. Documentation Reviewed: POL-01 Data Security Policies and Procedures					
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
3.7 Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are: ● Documented, ● In use, and ● Known to all affected parties	**Identify the document** reviewed to verify that security policies and operational procedures for protecting stored cardholder data are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for protecting stored cardholder data are: ● In use ● Known to all affected parties	Alex Umansky - Senior Software Engineer					

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: ● Only trusted keys and certificates are accepted. ● The protocol in use only supports secure versions or configurations. ● The encryption strength is appropriate for the encryption methodology in use. *Examples of open, public networks include but are not limited to:* ● *The Internet* ● *Wireless technologies, including 802.11 and Bluetooth* ● *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* ● *General Packet Radio Service (GPRS)* ● *Satellite communications*			☒	☐	☐	☐	☐
4.1.a Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.	**Identify** all locations where cardholder data is transmitted or received over open, public networks.	360 Advanced noted that the Fairfax CDE is hosted within AWS and that there are no wireless technologies applicable within the CDE. 360 Advanced also confirmed the existence of a bastion host (jump/management server) located in DMZ and used only for logical management access to the CDE. The bastion server utilizes SSH access. For a user to access a system within the CDE, another session needs to be created utilizing a combination of user ID and password. CHD is transmitted/received using the following services: Tokenization (HTTPS - Authorize.net)					
	Identify the documented standards examined.	POL-01 Data Security Policies and Procedures					
	Describe how the documented standards and system configurations both verified the use of:						
	● Security protocols for all locations	360 Advanced inspected running services, penetration testing results, and Qualys SSL Labs scans to verify that security protocols were in use. 360 Advanced noted that HTTPS and SFTP was used instead of insecure protocols such as HTTP and FTP. Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data AS-02.1 External & Internal Pen Test & Remediation SRV-01.3 Server Running Services & Listening Ports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Strong cryptography for all locations	360 Advanced inspected running services, penetration testing results, and Qualys SSL Labs scans to verify that security protocols were in use. 360 Advanced confirmed that support of strong cryptographic algorithms such as AES and SHA were enabled for the secure protocols in use. Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data AS-02.1 External & Internal Pen Test & Remediation SRV-01.3 Server Running Services & Listening Ports					
4.1.b Review documented policies and procedures to verify processes are specified for the following: ● For acceptance of only trusted keys and/or certificates. ● For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). ● For implementation of proper encryption strength per the encryption methodology in use.	**Identify the document** reviewed to verify that processes are specified for the following: ● For acceptance of only trusted keys and/or certificates. ● For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). ● For implementation of proper encryption strength per the encryption methodology in use.	POL-01 Data Security Policies and Procedures					
4.1.c Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit.	**Describe the sample** of inbound and outbound transmissions that were observed as they occurred.	Qualys SSL Labs scan results were analyzed for security and certificate information for Fairfax websites that were in scope.					
	Describe how the sample of inbound and outbound transmissions verified that all cardholder data is encrypted with strong cryptography during transit.	360 Advanced inspected penetration testing and Qualys SSL Labs scan results to verify that all inbound and outbound transmissions of cardholder data was encrypted with strong cryptography. Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data AS-02.1 External & Internal Pen Test & Remediation					
	For all instances where cardholder data is transmitted or received over open, public networks:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
4.1.d Examine keys and certificates to verify that only trusted keys and/or certificates are accepted.	**Describe the mechanisms** used to ensure that only trusted keys and/or certificates are accepted.	360 Advanced inspected website certificate information and observed the use of TLS certificates signed by trusted certificate authorities (CAs) to verify that only trusted keys and/or certificates were accepted. Certificate properties were verified to indicate valid certificate information. Navigating throughout the Fairfax websites did not warn the user of connecting to an invalid or untrusted certificate. In addition, penetration testing and Qualys SSL Labs scan results validated the use of these trusted certificate chains and public/private key pairs. Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data AS-02.1 External & Internal Pen Test & Remediation					
	Describe how the mechanisms were observed to accept only trusted keys and/or certificates.	360 Advanced inspected Qualys SSL Labs test scans and observed the use of TLS certificates signed by trusted CAs to verify that only trusted keys and/or certificates were accepted. Certificate properties were verified to indicate valid certificate information. In addition, penetration testing results validated the use of these trusted certificate chains and public/private key pairs. Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data AS-02.1 External & Internal Pen Test & Remediation					
4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.	*For all instances where cardholder data Is transmitted or received over open, public networks,* **describe how** system configurations verified that the protocol:						
	● Is implemented to use only secure configurations.	360 Advanced inspected penetration test reports and Qualys SSL Labs scan results to verify that protocols implemented used only secure configurations. Fairfax implemented industry-standard TLS v1.2 configurations considered to be secure. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation APP-01.3 Application - Encrypt Transmission of Sensitive Data					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Does not support insecure versions or configurations.	360 Advanced inspected penetration test reports and Qualys SSL Labs scan results to verify that protocols implemented did not support insecure versions or configurations. Results indicated that support for SSL and early TLS (including the use of weak TLS algorithms) was disabled. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation APP-01.3 Application - Encrypt Transmission of Sensitive Data					
4.1.f Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	*For each encryption methodology in use,*						
	Identify vendor recommendations/best practices for encryption strength.	Fairfax followed Qualys SSL Labs recommendations for encryption strength. Qualys SSL Labs: https://www.ssllabs.com/ssltest/index.html					
	Identify the encryption strength observed to be implemented.	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA					
4.1.g For TLS implementations, examine system configurations to verify that TLS is	**Indicate whether** TLS is implemented to encrypt cardholder data over open, public networks. **(yes/no)** *If 'no,' mark the remainder of 4.1.g as 'not applicable.'*	Yes.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
enabled whenever cardholder data is transmitted or received. *For example, for browser-based implementations:* ● *"HTTPS" appears as the browser Universal Record Locator (URL) protocol; and* ● *Cardholder data is only requested if "HTTPS" appears as part of the URL.*	*If "yes," for all instances where TLS is used to encrypt cardholder data over open, public networks,* **describe how** system configurations verified that TLS is enabled whenever cardholder data is transmitted or received.	360 Advanced inspected system configurations and Qualys SSL Labs test scans to verify that protocols implemented used only secure configurations. Fairfax implemented industry-standard TLS v1.2 configurations considered to be secure. Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data AS-02.1 External & Internal Pen Test & Remediation SRV-01.3 Server Running Services & Listening Ports					
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.			☐	☐	☒	☐	☐
4.1.1 Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified: ● Industry best practices are used to implement strong encryption for authentication and transmission. ● Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission.	**Identify** all wireless networks transmitting cardholder data or connected to the cardholder data environment.	Not Applicable. Fairfax's CDE resided solely within their hosted infrastructure provided by AWS, a PCI-compliant Level-1 Service Provider, who prohibited wireless connections within the hosted infrastructure. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	Identify the documented standards examined.	Not Applicable. Fairfax's CDE resided solely within their hosted infrastructure provided by AWS, a PCI-compliant Level-1 Service Provider, who prohibited wireless connections within the hosted infrastructure. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	Describe how the documented standards and system configuration settings both verified the following for all wireless networks identified:						
	● Industry best practices are used to implement strong encryption for authentication and transmission.	Not Applicable. Fairfax's CDE resided solely within their hosted infrastructure provided by AWS, a PCI-compliant Level-1 Service Provider, who prohibited wireless connections within the hosted infrastructure. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Weak encryption is not used as a security control for authentication or transmission.	Not Applicable. Fairfax's CDE resided solely within their hosted infrastructure provided by AWS, a PCI-compliant Level-1 Service Provider, who prohibited wireless connections within the hosted infrastructure. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).			☒	☐	☐	☐	☐
4.2.a If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	**Indicate whether** end-user messaging technologies are used to send cardholder data. **(yes/no)**	No.					
	If "no," mark the remainder of 4.2.a as "Not Applicable" and proceed to 4.2.b. *If "yes," complete the following:*						
	Describe how processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	Not Applicable. Fairfax prohibits the transmission of cardholder data via end-user messaging technologies. In addition, there are no system or end-user interfaces that display or output full PAN to be saved or sent.					
	Describe the sample of outbound transmissions that were observed as they occurred.	Not Applicable. Fairfax prohibits the transmission of cardholder data via end-user messaging technologies. In addition, there are no system or end-user interfaces that display or output full PAN to be saved or sent.					
	Describe how the sample of outbound transmissions verified that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	Not Applicable. Fairfax prohibits the transmission of cardholder data via end-user messaging technologies. In addition, there are no system or end-user interfaces that display or output full PAN to be saved or sent.					
4.2.b Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	**Identify the policy document** that prohibits PAN from being sent via end-user messaging technologies under any circumstances.	POL-01 Data Security Policies and Procedures					
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
4.3 Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:	**Identify the document** reviewed to verify that security policies and operational procedures for encrypting transmissions of cardholder data are documented.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Documented, • In use, and • Known to all affected parties.	**Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for encrypting transmissions of cardholder data are: • In use • Known to all affected parties	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).			☒	☐	☐	☐	☐
5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	**Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure.	Sample Set-1: Servers Sample Set-2: Administrator Laptops					
	For each item in the sample, **describe how** anti-virus software was observed to be deployed.	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus software was deployed to systems in the cardholder data environment. All anti-virus clients communicate to a centralized management server for software and definition updates. In addition, policies are pushed out to enforce scan schedules, scan actions, and to prevent the disabling of the anti-virus software itself. Status updates and log information are also sent to provide administrative oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-01 Server AV - Running & Prevent Disabling AV-02 Server AV - Update Schedule AV-03 Server AV - Scan Schedule AV-04 Server AV - Detection Action PC-03.1 PC AV - Running & Prevent Disabling PC-03.2 PC AV - Update Schedule PC-03.3 PC AV - Scan Schedule					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.			☒	☐	☐	☐	☐
5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs; ● Detect all known types of malicious software, ● Remove all known types of malicious software, and ● Protect against all known types of malicious software. *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).*	**Identify the vendor documentation** reviewed to verify that anti-virus programs: ● Detect all known types of malicious software, ● Remove all known types of malicious software, and ● Protect against all known types of malicious software.	Trend Micro Business Support - Deep Security 10.2: https://success.trendmicro.com/product-support/deep-security-10-2 McAfee LiveSafe - https://www.mcafee.com/consumer/en-us/store/m0/catalog/mls_430/mcafee-livesafe.html					
	Describe how anti-virus configurations verified that anti-virus programs:						
	● Detect all known types of malicious software,	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus agents were configured to detect all known types of malicious software. All anti-virus clients communicate to a centralized management server for software and definition updates. In addition, policies are pushed out to enforce scan schedules, scan actions, and to prevent the disabling of the anti-virus software itself. Status updates and log information are also sent to provide administrative oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-04 Server AV - Detection Action PC-03.4 PC AV - Detection Action					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Remove all known types of malicious software, and	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus agents were configured to quarantine or remove all malicious software upon detection. All anti-virus clients communicate to a centralized management server for software and definition updates. In addition, policies are pushed out to enforce scan schedules, scan actions, and to prevent the disabling of the anti-virus software itself. Status updates and log information are also sent to provide administrative oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-02 Server AV - Update Schedule AV-04 Server AV - Detection Action PC-03.2 PC AV - Update Schedule PC-03.4 PC AV - Detection Action					
	• Protect against all known types of malicious software.	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus agents were configured for real-time protection and to remove all known malicious software upon detection. All anti-virus clients communicate to a centralized management server for software and definition updates. In addition, policies are pushed out to enforce scan schedules, scan actions, and to prevent the disabling of the anti-virus software itself. Status updates and log information are also sent to provide administrative oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-01 Server AV - Running & Prevent Disabling AV-02 Server AV - Update Schedule AV-03 Server AV - Scan Schedule PC-03.1 PC AV - Running & Prevent Disabling PC-03.2 PC AV - Update Schedule PC-03.3 PC AV - Scan Schedule					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.			☒	☐	☐	☐	☐
5.1.2 Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.	**Identify the responsible personnel** interviewed for this testing procedure.	Alex Umansky - Senior Software Engineer Robert Castello - Director of Support Services					
	For the interview, **summarize the relevant details discussed** to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, and that such systems continue to not require anti-virus software.	360 Advanced inquired of responsible personnel to verify that changes in malware threats were monitored and evaluated. Personnel described how all machines were treated as having the same risk of being affected and deployed anti-virus software to all in-scope operating systems.					
5.2 Ensure that all anti-virus mechanisms are maintained as follows: ● Are kept current. ● Perform periodic scans. ● Generate audit logs which are retained per PCI DSS Requirement 10.7.			☒	☐	☐	☐	☐
5.2.a Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up-to-date.	**Identify the documented policies and procedures** examined to verify that anti-virus software and definitions are required to be kept up to date.	POL-01 Data Security Policies and Procedures					
5.2.b Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are: ● Configured to perform automatic updates, and ● Configured to perform periodic scans.	**Describe how** anti-virus configurations, including the master installation of the software, verified anti-virus mechanisms are:						
	● Configured to perform automatic updates, and	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus agents were configured to periodically poll for automated updates to anti-virus definition files. All anti-virus clients communicate to a centralized management server for software and definition updates. Status updates and log information are also sent to provide client oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-02 Server AV - Update Schedule PC-03.2 PC AV - Update Schedule					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Configured to perform periodic scans.	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus agents were configured to periodically perform an anti-virus scan. All anti-virus clients communicate to a centralized management server for software and definition updates. Status updates and log information are also sent to provide client oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-03 Server AV - Scan Schedule PC-03.3 PC AV - Scan Schedule					
5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: ● The anti-virus software and definitions are current. ● Periodic scans are performed.	**Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure.	Sample Set-1: Servers Sample Set-2: Administrator Laptops					
	Describe how the system components verified that:						
	● The anti-virus software and definitions are current.	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus agents were configured to periodically poll for automated updates to the anti-virus definition files. The definition version indicated a last update of the current date of when the observation was made. All anti-virus clients communicate to a centralized management server for software and definition updates. Status updates and log information are also sent to provide client oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-02 Server AV - Update Schedule PC-03.2 PC AV - Update Schedule					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Periodic scans are performed.	360 Advanced inspected anti-virus configuration settings and observed the status for each of the sampled devices to verify that anti-virus agents were configured to periodically perform an anti-virus scan. Scan policies were configured to perform active scanning every day. All anti-virus clients communicate to a centralized management server for software and definition updates. Status updates and log information are also sent to provide client oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: AV-03 Server AV - Scan Schedule PC-03.3 PC AV - Scan Schedule					
5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that: ● Anti-virus software log generation is enabled, and ● Logs are retained in accordance with PCI DSS Requirement 10.7.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers Sample Set-2: Administrator Laptops					
	For each item in the sample, **describe how** anti-virus configurations, including the master installation of the software, verified that:						
	● Anti-virus software log generation is enabled, and.	360 Advanced inspected log data generated by the anti-virus software for each of the sampled devices to verify that anti-virus agents were configured to generate log records. All anti-virus clients communicate to a centralized management server for software and definition updates. Status updates and log information are also sent to provide client oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples					
	● Logs are retained in accordance with PCI DSS Requirement 10.7.	360 Advanced inspected log data generated by the anti-virus software for each of the sampled devices to verify that anti-virus log records were retained for at least a year in accordance to Requirement 10.7. All anti-virus clients communicate to a centralized management server for software and definition updates. Status updates and log information are also sent to provide client oversight and reporting capabilities such as health state, virus definition version, anti-virus status, and last scan time. Documentation Reviewed: LOG-02 Central Log System - Log Retention					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*			☒	☐	☐	☐	☐
5.3.a Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers Sample Set-2: Administrator Laptops					
	For each item in the sample, **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software is actively running.	360 Advanced inspected anti-virus configuration settings and a list of active services for each of the sampled devices to verify that anti-virus agents were configured to run automatically upon system start up. Documentation Reviewed: AV-01 Server AV - Running & Prevent Disabling PC-03.1 PC AV - Running & Prevent Disabling SRV-01.1 Server User Listing & Access Permissions					
5.3.b Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users.	*For each item in the sample from 5.3.a,* **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software cannot be disabled or altered by users.	360 Advanced inspected anti-virus configuration settings and operating system group permissions and memberships for each of the sampled devices to verify that only IT administrators possessed the permission to alter the state of the anti-virus services. A demonstration was also performed to verify that the option to disable virus and spyware protection features were greyed out. Documentation Reviewed: AV-01 Server AV - Running & Prevent Disabling PC-03.1 PC AV - Running & Prevent Disabling SRV-01.1 Server User Listing & Access Permissions					
5.3.c Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by	**Identify the responsible personnel** interviewed who confirm that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Alex Umansky - Senior Software Engineer Robert Castello - Director of Support Services					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
management on a case-by-case basis for a limited time period.	**Describe how** processes were observed to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	360 Advanced inspected anti-virus configuration settings and operating system group permissions and memberships for each of the sampled devices to verify that non-privileged users did not possess the permission to alter the state of the anti-virus services. A demonstration was also performed to verify that the option to disable virus and spyware protection features were greyed out. Documentation Reviewed: AV-01 Server AV - Running & Prevent Disabling PC-03.1 PC AV - Running & Prevent Disabling SRV-01.1 Server User Listing & Access Permissions					
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
5.4 Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are: ● Documented, ● In use, and ● Known to all affected parties.	**Identify the document reviewed to** verify that security policies and operational procedures for protecting systems against malware are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for protecting systems against malware are: ● In use ● Known to all affected parties	Alex Umansky - Senior Software Engineer					

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*			☒	☐	☐	☐	☐
6.1.a Examine policies and procedures to verify that processes are defined for the following: ● To identify new security vulnerabilities. ● To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. ● To include using reputable outside sources for security vulnerability information.	**Identify the documented policies and procedures** examined to confirm that processes are defined: ● To identify new security vulnerabilities. ● To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. ● To include using reputable outside sources for security vulnerability information.	POL-01 Data Security Policies and Procedures					
6.1.b Interview responsible personnel and observe processes to verify that: ● New security vulnerabilities are identified. ● A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities. ● Processes to identify new security vulnerabilities include using reputable	**Identify the responsible personnel** interviewed who confirm that: ● New security vulnerabilities are identified. ● A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities. ● Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	Alex Umansky - Senior Software Engineer					
	Describe the processes observed to verify that:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
outside sources for security vulnerability information.	● New security vulnerabilities are identified.	360 Advanced observed that system administrators monitored a variety of industry patch and vulnerability notification websites, vendor newsletters, and mailing lists. 360 Advanced also noted that Fairfax performed annual penetration tests and quarterly vulnerability scans to identify and remediate new vulnerabilities that may potentially impact information security. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation SCN-01 Internal Vulnerability Scans SCN-02 External Vulnerability Scans					
	● A risk ranking is assigned to vulnerabilities to include identification of all "high" risk and "critical" vulnerabilities.	360 Advanced discussed the vulnerability management process with responsible personnel and was informed that risk rankings of low, medium, and high were applied based upon CVSS scores provided by vendor and industry-specific security bulletins. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation SCN-01 Internal Vulnerability Scans SCN-02 External Vulnerability Scans					
	● Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	360 Advanced observed that system administrators monitored a variety of industry patch and vulnerability notification websites, vendor newsletters, and mailing lists.					
	Identify the outside sources used.	Mitre - https://cve.mitre.org/ Amazon - http://blogs.aws.amazon.com/security/ Django - https://docs.djangoproject.com/en/dev/internals/security Microsoft Security Advisories and Bulletins - https://docs.microsoft.com/en-us/security-updates/ Nginx - http://nginx.org/en/security_advisories.html NIST NVD - https://nvd.nist.gov/vuln/data-feeds Openssl - https://www.openssl.org/news/vulnerabilities.html US-CERT - https://www.us-cert.gov/ncas/alerts					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:*** *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*			☒	☐	☐	☐	☐
6.2.a Examine policies and procedures related to security-patch installation to verify processes are defined for: ● Installation of applicable critical vendor-supplied security patches within one month of release. ● Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).	**Identify the documented policies and procedures** related to security-patch installation examined to verify processes are defined for: ● Installation of applicable critical vendor-supplied security patches within one month of release. ● Installation of all applicable vendor-supplied security patches within an appropriate time frame.	POL-01 Data Security Policies and Procedures					
6.2.b For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following: ● That applicable critical vendor-supplied security patches are installed within one month of release. ● All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).	**Identify the sample** of system components and related software selected for this testing procedure.	Sample Set-1: Servers					
	Identify the vendor security patch list reviewed.	Windows Security Advisories: https://technet.microsoft.com/en-us/security/dd252948.aspx					
	For each item in the sample, **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify that:						
	● Applicable critical vendor-supplied security patches are installed within one month of release.	360 Advanced inspected system patch history to verify that critical security patches were installed within one month of vendor release. Critical updates identified are installed and incorporated within the baseline Amazon Machine Image and affected servers are destroyed and redeployed using the updated image. In addition, Trend Micro Deep Security agents were installed on systems to shield potential vulnerabilities until a patch is made available and deployed or in place of a future patch that may never materialize. Documentation Reviewed: CHG-02 Change Records - System Changes SRV-01.5 Server Patch Updates Installed & Settings					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• All applicable vendor-supplied security patches are installed within an appropriate time frame.	360 Advanced inspected system patch history to verify that all applicable security patches were installed within an appropriate time frame. Critical updates identified are installed and incorporated within the baseline Amazon Machine Image and affected servers are destroyed and redeployed using the updated image. In addition, Trend Micro Deep Security agents were installed on systems to shield potential vulnerabilities until a patch is made available and deployed or in place of a future patch that may never materialize. Documentation Reviewed: CHG-02 Change Records - System Changes SRV-01.5 Server Patch Updates Installed & Settings					
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging). • Based on industry standards and/or best practices. • Incorporate information security throughout the software development life cycle. ***Note:*** *this applies to all software developed internally as well as bespoke or custom software developed by a third party.*			☒	☐	☐	☐	☐
6.3.a Examine written software-development processes to verify that the processes are based on industry standards and/or best practices.	**Identify the document** examined to verify that software-development processes are based on industry standards and/or best practices.	POL-01 Data Security Policies and Procedures					
6.3.b Examine written software development processes to verify that information security is included throughout the life cycle.	**Identify the documented software development processes** examined to verify that information security is included throughout the life cycle.	POL-01 Data Security Policies and Procedures					
6.3.c Examine written software development processes to verify that software applications are developed in accordance with PCI DSS.	**Identify the documented software development processes** examined to verify that software applications are developed in accordance with PCI DSS.	POL-01 Data Security Policies and Procedures					
6.3.d Interview software developers to verify that written software development processes are implemented.	**Identify the software developers** interviewed who confirm that written software development processes are implemented.	Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.			☒	☐	☐	☐	☐
6.3.1 Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	**Identify the documented software-development processes** examined to verify processes define that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	Alex Umansky - Senior Software Engineer					
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: ● Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices. ● Code reviews ensure code is developed according to secure coding guidelines. ● Appropriate corrections are implemented prior to release. ● Code review results are reviewed and approved by management prior to release. ***Note:*** *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.3.2.a Examine written software development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows: ● Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ● Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). ● Appropriate corrections are implemented prior to release. ● Code-review results are reviewed and approved by management prior to release.	**Identify the documented software-development processes examined to verify processes** define that all custom application code changes must be reviewed (using either manual or automated processes) as follows: ● Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ● Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). ● Appropriate corrections are implemented prior to release. ● Code-review results are reviewed and approved by management prior to release.	POL-01 Data Security Policies and Procedures				
	Identify the responsible personnel interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows: ● Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. ● Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). ● Appropriate corrections are implemented prior to release. ● Code-review results are reviewed and approved by management prior to release.	Alex Umansky - Senior Software Engineer					
6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.	**Identify the sample** of recent custom application changes selected for this testing procedure.	CHG-03 Change Records - Application Changes Deployed to Production					
	For each item in the sample, **describe how** code review processes were observed to verify custom application code is reviewed as follows:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Code changes are reviewed by individuals other than the originating code author.	360 Advanced inspected a sample application change ticket to verify that changes included code review by individuals other than the originating author. The ticketing and project workflow included processes that documented the performance and completion of code review and the CAB approval of moving projects to the next phase. Documentation Reviewed: POL-01 Data Security Policies and Procedures CHG-03 Change Records - Application Changes Deployed to Production					
	● Code changes are reviewed by individuals who are knowledgeable in code-review techniques and secure coding practices.	360 Advanced inspected a sample application change ticket to verify that other developers familiar with code review and secure coding performed code reviews as part of the project workflow. Documentation Reviewed: POL-01 Data Security Policies and Procedures CHG-03 Change Records - Application Changes Deployed to Production					
	● Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5).	360 Advanced inspected a sample application change ticket to verify that processes included testing as part of the review, via a defined set of tests that examined for vulnerabilities, including those listed in PCI DSS Requirement 6.5. Documentation Reviewed: POL-01 Data Security Policies and Procedures CHG-03 Change Records - Application Changes Deployed to Production					
	● Appropriate corrections are implemented prior to release.	Although the sampled projects did not contain corrections, 360 Advanced inspected documented software development procedures and walked through the testing and re-routing workflow, to verify that an orderly development life cycle was followed that included implementation of appropriate corrections to errors discovered during testing prior to releasing applications to production. Documentation Reviewed: POL-01 Data Security Policies and Procedures CHG-03 Change Records - Application Changes Deployed to Production					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Code-review results are reviewed and approved by management prior to release.	360 Advanced inspected a sample application change ticket to verify that management/CAB approval was required to be documented in the ticket workflow prior to releasing applications to production. Documentation Reviewed: POL-01 Data Security Policies and Procedures CHG-03 Change Records - Application Changes Deployed to Production					
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:			☒	☐	☐	☐	☐
6.4 Examine policies and procedures to verify the following are defined: • Development/test environments are separate from production environments with access control in place to enforce separation. • A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. • Production data (live PANs) are not used for testing or development. • Test data and accounts are removed before a production system becomes active. • Change control procedures related to implementing security patches and software modifications are documented.	**Identify the documented policies and procedures** examined to verify that the following are defined: • Development/test environments are separate from production environments with access control in place to enforce separation. • A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. • Production data (live PANs) are not used for testing or development. • Test data and accounts are removed before a production system becomes active. • Change-control procedures related to implementing security patches and software modifications are documented.	POL-01 Data Security Policies and Procedures				
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.			☒	☐	☐	☐	☐
6.4.1.a Examine network documentation and network device configurations to verify that the development/test	**Identify the network documentation** examined to verify that the development/test environments are separate from the production environment(s).	DGM-01 Network Diagrams DGM-02 Data Flow Diagrams					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
environments are separate from the production environment(s).	**Describe how** network device configurations verified that the development/test environments are separate from the production environment(s).	360 Advanced inquired of responsible personnel to verify that development/test environments are separate from the production environment. Personnel described that production and development environments reside on separate AWS VPCs with no connectivity between them. Documentation Reviewed: DGM-02 Data Flow Diagrams					
6.4.1.b Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s).	**Identify the access control settings** examined for this testing procedure.	AWS-01 AWS IAM - User Listing & Access Permissions & MFA DB-01 Database User Listing & Access Permissions DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
	Describe how the access control settings verified that access controls are in place to enforce separation between the development/test environments and the production environment(s).	360 Advanced inspected access control settings on test and production systems to verify that developers did not have access to the production cardholder data environment. Application changes were deployed by IT administrators and not by the developers themselves.					
6.4.2 Separation of duties between development/test and production environments.			☒	☐	☐	☐	☐
6.4.2 Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment.	**Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment.	Alex Umansky - Senior Software Engineer					
	Identify the personnel assigned to production environments interviewed who confirm that separation of duties is in place between development/test environments and the production environment.	Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how processes were observed to verify that separation of duties is in place between development/test environments and the production environment.	360 Advanced inspected access control settings on test and production systems to verify that developers did not have access to the production CDE and that only designated systems personnel were permitted privileged access to deploy code into the production environment. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DB-01 Database User Listing & Access Permissions DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
6.4.3 Production data (live PANs) are not used for testing or development.			☒	☐	☐	☐	☐
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	**Identify the responsible personnel** interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	Alex Umansky - Senior Software Engineer					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	360 Advanced inspected database contents to verify that live PANs were not used for testing. Fairfax uses tokenization for processing credit card transactions and does not store or process PANs. There is no testing of PANs in development testing. Documentation Reviewed: DB-04 Database Schema Listing DEV-04 Sanitization Between Test & Production Environments					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	360 Advanced inspected database contents to verify that live PANs were not used for development. Fairfax uses tokenization for processing credit card transactions and does not store or process PANs. There is no testing of PANs in development testing. Documentation Reviewed: DB-04 Database Schema Listing DEV-04 Sanitization Between Test & Production Environments					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	**Describe how** a sample of test data was examined to verify production data (live PANs) is not used for testing.	360 Advanced inspected database contents to verify that live PANs were not used for testing. Fairfax uses tokenization for processing credit card transactions and does not store or process PANs. There is no testing of PANs in development testing. Documentation Reviewed: DB-04 Database Schema Listing DEV-04 Sanitization Between Test & Production Environments					
	Describe how a sample of test data was examined to verify production data (live PANs) is not used for development.	360 Advanced inspected database contents to verify that live PANs were not used for development. Fairfax uses tokenization for processing credit card transactions and does not store or process PANs. There is no testing of PANs in development testing. Documentation Reviewed: DB-04 Database Schema Listing DEV-04 Sanitization Between Test & Production Environments					
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.			☒	☐	☐	☐	☐
6.4.4.a Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active.	**Identify the responsible personnel** interviewed who confirm that test data and accounts are removed before a production system becomes active.	Alex Umansky - Senior Software Engineer					
	Describe how testing processes were observed to verify that test data is removed before a production system becomes active.	360 Advanced inquired of responsible personnel to verify that test data was removed before a production system became active. Personnel demonstrated the testing and deployment processes and described how test/development environments are based on the production infrastructure build pipeline. Approved changes are incorporated into the production build pipeline and deployed as a new instance instead of deploying changes within the existing production instance. Documentation Reviewed: DEV-02 Integration & Deployment Tools - User Listing & Permissions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how testing processes were observed to verify that test accounts are removed before a production system becomes active.	360 Advanced inquired of responsible personnel to verify that test accounts were removed before a production system became active. Personnel demonstrated the testing and deployment processes and described how test/development environments are based on the production infrastructure build pipeline. Approved changes are incorporated into the production build pipeline and deployed as a new instance instead of deploying changes within the existing production instance. Documentation Reviewed: DEV-02 Integration & Deployment Tools - User Listing & Permissions					
6.4.4.b Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.	**Describe how** the sampled data examined verified that test data is removed before the system becomes active.	360 Advanced inquired of responsible personnel to verify that test data was removed before a production system became active. Personnel demonstrated the testing and deployment processes and described how test/development environments are based on the production infrastructure build pipeline. Approved changes are incorporated into the production build pipeline and deployed as a new instance instead of deploying changes within the existing production instance. Documentation Reviewed: DEV-02 Integration & Deployment Tools - User Listing & Permissions					
	Describe how the sampled data examined verified that test accounts are removed before the system becomes active.	360 Advanced inquired of responsible personnel to verify that test accounts were removed before a production system became active. Personnel demonstrated the testing and deployment processes and described how test/development environments are based on the production infrastructure build pipeline. Approved changes are incorporated into the production build pipeline and deployed as a new instance instead of deploying changes within the existing production instance. Documentation Reviewed: DEV-02 Integration & Deployment Tools - User Listing & Permissions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.5 Change control procedures must include the following:			☒	☐	☐	☐	☐
6.4.5.a Examine documented change-control procedures and verify procedures are defined for: ● Documentation of impact. ● Documented change approval by authorized parties. ● Functionality testing to verify that the change does not adversely impact the security of the system. ● Back-out procedures.	**Identify the documented change-control procedures** examined to verify procedures are defined for: ● Documentation of impact. ● Documented change approval by authorized parties. ● Functionality testing to verify that the change does not adversely impact the security of the system. ● Back-out procedures.	POL-01 Data Security Policies and Procedures					
6.4.5.b For a sample of system components, interview responsible personnel to determine recent changes. Trace those changes back to related change control documentation. For each change examined, perform the following:	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	Identify the responsible personnel interviewed to determine recent changes.	Alex Umansky - Senior Software Engineer					
	For each item in the sample, **identify the sample** of changes and the related change control documentation selected for this testing procedure (through 6.4.5.4).	All infrastructure and code changes follow the same change management policies and procedures that require documentation and testing as defined by this requirement. Network Changes CHG-01 Change Records - Network Changes System Changes CHG-02 Change Records - System Changes Application Changes CHG-03 Change Records - Application Changes Deployed to Production					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.5.1 Documentation of impact.			☒	☐	☐	☐	☐
6.4.5.1 Verify that documentation of impact is included in the change control documentation for each sampled change.	*For each change from 6.4.5.b*, **describe how** the documentation of impact is included in the change control documentation for each sampled change.	360 Advanced inspected a sample of change request tickets to verify that documentation was included on each ticket describing the functional changes related to the project and the impact of these changes. This also matched the stated development life cycle requirements described in the software development methodology documentation. Documentation Reviewed: POL-01 Data Security Policies and Procedures					
6.4.5.2 Documented change approval by authorized parties.			☒	☐	☐	☐	☐
6.4.5.2 Verify that documented approval by authorized parties is present for each sampled change.	*For each change from 6.4.5.b*, **describe how** documented approval by authorized parties is present in the change control documentation for each sampled change.	360 Advanced inspected a sample of change request tickets to verify that documentation was included on each ticket indicating explicit approval of changes by authorized management. This also matched the stated development life cycle requirements described in the software development methodology documentation. Documentation Reviewed: POL-01 Data Security Policies and Procedures					
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.			☒	☐	☐	☐	☐
6.4.5.3.a For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.	*For each change from 6.4.5.b*, **describe how** the change control documentation confirmed that functionality testing is performed to verify that the change does not adversely impact the security of the system.	360 Advanced inspected a sample of change request tickets to verify that documentation was included on each ticket within the Request Tracker ticketing and project management software describing functionality and security testing at multiple stages of the project workflow, passing a project to the next phase only upon successful completion of testing. This also matched the stated development life cycle requirements described in the software development methodology documentation. Documentation Reviewed: POL-01 Data Security Policies and Procedures					
6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	For each item in the sample, **identify the sample** of custom code changes and the related change control documentation selected for this testing procedure.	CHG-03 Change Records - Application Changes Deployed to Production					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	For each change, **describe how** the change control documentation verified that updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	360 Advanced inspected a sample of change request tickets to verify that documentation was included on each ticket describing code review and/or testing for application vulnerabilities, including those listed in PCI DSS Requirement 6.5, as part of the review and documented workflow. This also matched the stated development life cycle requirements described in the software development methodology documentation. Documentation Reviewed: POL-01 Data Security Policies and Procedures					
6.4.5.4 Back-out procedures.			☒	☐	☐	☐	☐
6.4.5.4 Verify that back-out procedures are prepared for each sampled change.	*For each change from 6.4.5.b*, **describe how** the change control documentation verified that back-out procedures are prepared.	360 Advanced inspected a sample of change request tickets to verify that documentation was included that detailed back-out procedures as part of the documented workflow. 360 Advanced noted that each sampled project ticket included a detailed listing of all new or updated code, as well as any relevant database changes, which enabled system administrators to quickly rollback to previous versions from the Subversion (SVN) repository. This also matched the stated development life cycle requirements described in the software development methodology documentation. Documentation Reviewed: POL-01 Data Security Policies and Procedures					
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.			☒	☐	☐	☐	☐
6.4.6 For a sample of significant changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	**Identify whether** a significant change occurred within the past 12 months. **(yes/no)** *If "yes," complete the following:* *If "no," mark the rest of 6.4.6 as "Not Applicable"*	Yes.					
	Identify the responsible personnel interviewed for this testing procedure.	Alex Umansky - Senior Software Engineer					
	Identify the relevant documentation reviewed to verify that the documentation was updated as part of the change.	DGM-01 Network Diagrams DGM-02 Data Flow Diagrams NET-00 Inventory of Network Devices in Scope SRV-00 Inventory of Servers in Scope					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the sample of change records examined for this testing procedure.	CHG-05 Change Records - Significant Changes to Environment					
	Identify the sample of systems/networks affected by the significant change.	Sample Set-3 File Servers Sample Set-4 Web Servers Sample Set-5 Domain Controllers / NTP Servers					
	For each sampled change, **describe how** the system/networks observed verified that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	Change request tickets documented the pre-migration process and cutover procedures. All relevant diagrams, system inventories, and procedures were noted to be updated to reflect the new TierPoint environment.					
6.5 Address common coding vulnerabilities in software-development processes as follows: ● Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. ● Develop applications based on secure coding guidelines. ***Note:*** *The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*			☒	☐	☐	☐	☐
6.5.a Examine software development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers at least annually, based on industry best practices and guidance.	**Identify the document** reviewed to verify that up-to-date training in secure coding techniques is required for developers at least annually.	POL-01 Data Security Policies and Procedures					
	Identify the industry best practices and guidance on which the training is based.	The Open Web Application Security Project (OWASP) - http://www.owasp.org National Institute of Standards Technology (NIST) - http://www.nist.gov					
6.5.b Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities	**Identify the records of training** that were examined to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities.	TRN-02 Developer Secure Coding Training					
6.5.c. Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities:	**Identify the software-development policies and procedures** examined to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10.	Alex Umansky - Senior Software Engineer					
Note: *Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external):*							
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.			☒	☐	☐	☐	☐
6.5.1 Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include: ● Validating input to verify user data cannot modify meaning of commands and queries. ● Utilizing parameterized queries.	*For the interviews at 6.5.d*, **summarize the relevant details** discussed to verify that injection flaws are addressed by coding techniques that include:						
	● Validating input to verify user data cannot modify meaning of commands and queries.	360 Advanced inquired of responsible personnel and inspected software development documentation to verify that injection flaws were addressed by secure coding techniques. Code reviewers manually performed tests in line with recommendations from the OWASP guidelines to examine application code for protection against injection attacks, including input validation. 360 Advanced also noted that annual web application penetration testing is performed to detect and AWS web application firewalls were configured to actively block several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Utilizing parameterized queries.	360 Advanced inquired of responsible personnel and inspected software development documentation to verify that injection flaws were addressed by secure coding techniques. Code reviewers manually performed tests to examine application code for protection against injection attacks, including the use of parameterized queries. 360 Advanced also noted that annual web application penetration testing is performed to detect and AWS web application firewalls were configured to actively block several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					
6.5.2 Buffer overflow.			☒	☐	☐	☐	☐
6.5.2 Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include: • Validating buffer boundaries. • Truncating input strings.	*For the interviews at 6.5.d*, **summarize the relevant details** discussed to verify that buffer overflows are addressed by coding techniques that include:						
	• Validating buffer boundaries.	360 Advanced inquired of responsible personnel and inspected software development documentation to verify that injection flaws were addressed by secure coding techniques. Code reviewers manually performed tests to examine application code for protection against injection attacks, including the use of parameterized queries. 360 Advanced also noted that annual web application penetration testing is performed to detect and AWS web application firewalls were configured to actively block several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Truncating input strings.	360 Advanced inquired of responsible personnel and inspected software development documentation to verify that injection flaws were addressed by secure coding techniques. Code reviewers manually performed tests to examine application code for protection against injection attacks, including the use of parameterized queries. 360 Advanced also noted that annual web application penetration testing is performed to detect and AWS web application firewalls were configured to actively block several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					
6.5.3 Insecure cryptographic storage.			☒	☐	☐	☐	☐
6.5.3 Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that: • Prevent cryptographic flaws. • Use strong cryptographic algorithms and keys.	*For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that insecure cryptographic storage is addressed by coding techniques that:						
	• Prevent cryptographic flaws.	360 Advanced inquired of responsible personnel and inspected software development documentation to verify that injection flaws were addressed by secure coding techniques. Code reviewers manually performed tests to examine application code for protection against injection attacks, including the use of parameterized queries. 360 Advanced also noted that annual web application penetration testing is performed to detect several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Use strong cryptographic algorithms and keys.	360 Advanced inquired of responsible personnel and inspected software development documentation to verify that injection flaws were addressed by secure coding techniques. Code reviewers manually performed tests to examine application code for protection against injection attacks, including the use of parameterized queries. 360 Advanced also noted that annual web application penetration testing is performed to detect several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
6.5.4 Insecure communications.			☒	☐	☐	☐	☐
6.5.4 Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications.	*For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that insecure communications are addressed by coding techniques that properly:						
	• Authenticate all sensitive communications.	360 Advanced inquired of key personnel and inspected software development documentation to verify that insecure communications were addressed by secure coding techniques that authenticate all sensitive communications. Code reviewers manually reviewed affected pages to verify that they required the use of secure protocols and encryption algorithms in addition to reviewing periodic ASV and internal vulnerability scans to ensure secure authentication and encryption of all sensitive communications. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures SCN-01 Internal Vulnerability Scans SCN-02 External Vulnerability Scans					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Encrypt all sensitive communications.	360 Advanced inquired of key personnel and inspected software development documentation to verify that insecure communications were addressed by secure coding techniques that authenticate all sensitive communications. Code reviewers manually reviewed affected pages to verify that they required the use of secure protocols and encryption algorithms in addition to reviewing periodic ASV and internal vulnerability scans to ensure secure authentication and encryption of all sensitive communications. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures SCN-01 Internal Vulnerability Scans SCN-02 External Vulnerability Scans					
6.5.5 Improper error handling.			☒	☐	☐	☐	☐
6.5.5 Examine-software development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details).	*For the interviews at 6.5.d*, **summarize the relevant details** discussed to verify that improper error handling is addressed by coding techniques that do not leak information via error messages.	360 Advanced inquired of key personnel and inspected software development documentation to verify that improper error handling was addressed by secure coding techniques. Code reviewers manually performed tests to ensure application code utilized structured error handling and only responded with messages that did not provide any sensitive information or messages to end users. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).			☒	☐	☐	☐	☐
6.5.6 Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.	*For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.	External sources and internal test results are routinely checked to identify vulnerabilities in application code. Once vulnerabilities are identified, a risk ranking based upon vendor recommendations and CVSS scores are applied, and performed manual tests to examine for susceptibility to these vulnerabilities during regression testing of each build, prior to deployment. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
Note: *Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):*							
Indicate whether web applications and application interfaces are present. **(yes/no)** *If "no," mark the below 6.5.7-6.5.10 as "Not Applicable."* *If "yes,"* ***complete the following:***		Yes.					
6.5.7 Cross-site scripting (XSS).			☒	☐	☐	☐	☐
6.5.7 Examine software-development policies and procedures and interview	*For the interviews at 6.5.d***, summarize the relevant details** discussed to verify that cross-site scripting (XSS) is addressed by coding techniques that include:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include: ● Validating all parameters before inclusion. ● Utilizing context-sensitive escaping.	● Validating all parameters before inclusion.	360 Advanced inquired of key personnel and inspected software development documentation to verify that cross-site scripting was addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for protection against cross-site scripting attacks, including validation of all parameters before inclusion. 360 Advanced also noted that annual web application penetration testing is performed to detect and AWS web application firewalls were configured to actively block several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					
	● Utilizing context-sensitive escaping.	360 Advanced inquired of key personnel and inspected software development documentation to verify that cross-site scripting was addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for protection against cross-site scripting attacks, including rejection of all included script tags and utilizing context-sensitive escaping. 360 Advanced also noted that annual web application penetration testing is performed to detect and AWS web application firewalls were configured to actively block several categories of these types of vulnerabilities. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).			☒	☐	☐	☐	☐
6.5.8 Examine software-development policies and procedures and interview	*For the interviews at 6.5.d*, **summarize the relevant details** discussed to verify that improper access control is addressed by coding techniques that include:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that include: ● Proper authentication of users. ● Sanitizing input. ● Not exposing internal object references to users. ● User interfaces that do not permit access to unauthorized functions.	● Proper authentication of users.	360 Advanced inquired of key personnel and inspected software development documentation to verify that cross-site scripting was addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for proper authentication of users, including restricting form authentication cookies to HTTPS connections and non-persistent storage. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
	● Sanitizing input.	360 Advanced inquired of key personnel and inspected software development documentation to verify that cross-site scripting was addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for sanitizing input, including restricting and validating input parameters to expected data types and length. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
	● Not exposing internal object references to users.	360 Advanced inquired of key personnel and inspected software development documentation to verify that cross-site scripting was addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for preventing exposure of internal object references in either the URL or page content. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• User interfaces that do not permit access to unauthorized functions.	360 Advanced inquired of key personnel and inspected software development documentation to verify that cross-site scripting was addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for preventing access to unauthorized functions via user interfaces, including ensuring that session tokens managed by web services did not persist beyond defined sessions or allowed users to access functions outside of defined roles. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
6.5.9 Cross-site request forgery (CSRF).			☒	☐	☐	☐	☐
6.5.9 Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	*For the interviews at 6.5.d*, **summarize the relevant details** discussed to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	360 Advanced inquired of key personnel and inspected software development documentation to verify that cross-site scripting was addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for preventing cross-site request forgery, including verifying the source and target origins with standard headers along with the use of CSRF tokens. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
6.5.10 Broken authentication and session management**.**			☒	☐	☐	☐	☐
6.5.10 Examine software development policies and procedures and interview	*For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that broken authentication and session management are addressed via coding techniques that commonly include:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include: ● Flagging session tokens (for example cookies) as "secure." ● Not exposing session IDs in the URL. ● Incorporating appropriate time-outs and rotation of session IDs after a successful login.	● Flagging session tokens (for example cookies) as "secure."	360 Advanced inquired of key personnel and inspected software development documentation to verify that broken authentication and session management were addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for protection against broken authentication and session management, including configuring session tokens as "secure" at the top level of the web server configuration with each child site properly inheriting this global setting. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
	● Not exposing session IDs in the URL.	360 Advanced inquired of key personnel and inspected software development documentation to verify that broken authentication and session management were addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for protection against broken authentication and session management, including using session IDs that are never exposed to users within URLs or over an unencrypted connection. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Incorporating appropriate time-outs and rotation of session IDs after a successful login.	360 Advanced inquired of key personnel and inspected software development documentation to verify that broken authentication and session management were addressed by secure coding techniques. Code reviewers manually reviewed code changes and performed tests in line with recommendations from the OWASP guidelines to examine application code for protection against broken authentication and session management, including a default timeout session for each web application and the use of new session IDs after a successful login. In addition, web application penetration testing was performed on an annual basis to ensure validation of secure coding practices based on the OWASP Top 10. Documentation Reviewed: AS-02.1 External & Internal Pen Test & Remediation POL-01 Data Security Policies and Procedures					
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: ● Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* ● Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.			☒	☐	☐	☐	☐
6.6 For *public-facing* web applications, ensure that either one of the following methods is in place as follows: ● Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: ● At least annually.	For each public-facing web application, **identify which** of the two methods are implemented: ● Web application vulnerability security assessments, AND/OR ● Automated technical solution that detects and prevents web-based attacks, such as web application firewalls.	Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	If application vulnerability security assessments are indicated above:						
	Describe the tools and/or methods used (manual or automated, or a combination of both).	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● After any changes. ● By an organization that specializes in application security. ● That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. ● That all vulnerabilities are corrected. ● That the application is re-evaluated after the corrections. ● Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: ● Is situated in front of public-facing web applications to detect and prevent web-based attacks. ● Is actively running and up-to-date as applicable. ● Is generating audit logs. ● Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	**Identify the documented processes** that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows: ● At least annually. ● After any changes. ● By an organization that specializes in application security. ● That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. ● That all vulnerabilities are corrected ● That the application is re-evaluated after the corrections.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	Identify the responsible personnel interviewed who confirm that public-facing web applications are reviewed, as follows: ● At least annually. ● After any changes. ● By an organization that specializes in application security. ● That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. ● That all vulnerabilities are corrected. ● That the application is re-evaluated after the corrections.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	Identify the records of application vulnerability security assessments examined for this testing procedure.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	Describe how the records of application vulnerability security assessments verified that public-facing web applications are reviewed as follows:						
	● At least annually.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● After any changes.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	● By an organization that specialized in application security.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	● That at a minimum, all vulnerabilities in requirement 6.5 are included in the assessment.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	● That all vulnerabilities are corrected.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	● That the application is re-evaluated after the corrections.	Not Applicable. Automated technical solutions using web application firewalls were used to detect and prevent web-based attacks for all public-facing web applications.					
	If an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is indicated above:						
	Describe the automated technical solution in use that detects and prevents web-based attacks.	Amazon Web Services Web Application Firewall services were used as a cloud-based web application firewall that inspected traffic prior to processing by the web application code. AWS WAF delivered real-time protection against a variety of web-based attacks and provided logging of malicious attempts. Documentation Reviewed: WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed who confirm that the above automated technical solution is in place as follows: ● Is situated in front of public-facing web applications to detect and prevent web-based attacks. ● Is actively running and up-to-date as applicable. ● Is generating audit logs. ● Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	Alex Umansky - Senior Software Engineer					
	Describe how the system configuration settings verified that the above automated technical solution is in place as follows:						
	● Is situated in front of public-facing web applications to detect and prevent web-based attacks.	360 Advanced inspected web application firewall settings to verify that the Amazon Web Services Web Application Firewalls were configured and deployed to inspect and analyze web requests prior to processing and delivery to the websites to which they were directed. Documentation Reviewed: WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					
	● Is actively running and up-to-date as applicable.	360 Advanced inspected web application firewall settings to verify that the Amazon Web Services Web Application Firewalls were actively running and configured to start automatically. Documentation Reviewed: WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					
	● Is generating audit logs.	360 Advanced inspected web application firewall settings and observed sample audit log entries for detected attacks to verify that the Amazon Web Services Web Application Firewalls were configured to generate logs of attempted web attacks. Documentation Reviewed: WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	360 Advanced inspected web application firewall settings and observed web page block notifications of detected attacks to verify that the Amazon Web Services Web Application Firewalls were configured to block recognized attacks. Documentation Reviewed: WAF-01 WAF Configuration - Actively Running & Updated WAF-02 WAF Configuration - Block or Alert Rule Settings & Examples					
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
6.7 Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** examined to verify that security policies and operational procedures for developing and maintaining secure systems and applications are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for developing and maintaining secure systems and applications are: • In use • Known to all affected parties	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.			☒	☐	☐	☐	☐
7.1.a Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: ● Defining access needs and privilege assignments for each role. ● Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. ● Assignment of access based on individual personnel's job classification and function. ● Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	**Identify the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows: ● Defining access needs and privilege assignments for each role. ● Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. ● Assignment of access based on individual personnel's job classification and function ● Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	POL-01 Data Security Policies and Procedures					
7.1.1 Define access needs for each role, including: ● System components and data resources that each role needs to access for their job function. ● Level of privilege required (for example, user, administrator, etc.) for accessing resources.			☒	☐	☐	☐	☐
7.1.1 Select a sample of roles and verify access needs for each role are defined and include:	**Identify the selected sample** of roles for this testing procedure.	Senior Software Engineer System Administrators Software Developers					
	For each role in the selected sample, **describe how** the role was examined to verify access needs are defined and include:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● System components and data resources that each role needs to access for their job function. ● Identification of privilege necessary for each role to perform their job function.	● System components and data resources that each role needs to access for their job function.	360 Advanced inspected the responsibilities described in policy documents and job descriptions for each sampled role to verify that access needs for each role were defined and included system components and data resources needed for each role to perform their job functions. Documentation Reviewed: ORG-02 Job Descriptions POL-01 Data Security Policies and Procedures					
	● Identification of privilege necessary for each role to perform their job function.	360 Advanced inspected the responsibilities described in policy documents and job descriptions for each sampled role and compared them with user access configurations within system components to verify that each role was granted the access necessary to perform the job associated with that role and limited access as defined within documented privileges. Documentation Reviewed: POL-01 Data Security Policies and Procedures AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.			☒	☐	☐	☐	☐
7.1.2.a Interview personnel responsible for assigning access to verify that access to privileged user IDs is: ● Assigned only to roles that specifically require such privileged access. ● Restricted to least privileges necessary to perform job responsibilities.	**Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is: ● Assigned only to roles that specifically require such privileged access. ● Restricted to least privileges necessary to perform job responsibilities.	Alex Umansky - Senior Software Engineer					
7.1.2.b Select a sample of user IDs with privileged access and interview	**Identify the sample** of user IDs ***with privileged access*** selected for this testing procedure.	System Administrators					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
responsible management personnel to verify that privileges assigned are: ● Necessary for that individual's job function. ● Restricted to least privileges necessary to perform job responsibilities.	**Identify the responsible management personnel** interviewed to confirm that privileges assigned are: ● Necessary for that individual's job function. ● Restricted to least privileges necessary to perform job responsibilities.	Alex Umansky - Senior Software Engineer					
	For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are:						
	● Necessary for that individual's job function.	360 Advanced inquired of responsible personnel and inspected user access configurations to verify that privileges assigned to each sampled user ID were necessary for that individual's job function. Personnel explained that only IT administrators had access to components in the production CDE and that this access matched defined job functions. Documentation Reviewed: POL-01 Data Security Policies and Procedures AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
	● Restricted to least privileges necessary to perform job responsibilities.	360 Advanced inquired of responsible personnel and inspected user access configurations to verify that privileges assigned to each sampled user ID were restricted to the least privileges necessary to perform job responsibilities. Personnel explained that operating system and application access controls were used to limit access to only that necessary to perform job responsibilities. Documentation Reviewed: POL-01 Data Security Policies and Procedures AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
7.1.3 Assign access based on individual personnel's job classification and function.			☒	☐	☐	☐	☐
7.1.3 Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual's job classification and function.	**Identify the sample** of user IDs selected for this testing procedure.	Sample Set-3: New Hires A sample of user IDs assigned to new employees were selected and compared with the associated permissions for each system component. Assigned rights and privileges were found to be assigned based on the individual's job title indicated within the employee roster. Documentation Reviewed: EMP-00 Employee Roster					
	Identify the responsible management personnel interviewed who confirm that privileges assigned are based on that individual's job classification and function.	Alex Umansky - Senior Software Engineer					
	For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are based on that individual's job classification and function.	360 Advanced inquired of responsible personnel to verify that privileges assigned to each sampled user ID were necessary for that individual's job function. Personnel explained that only IT Administrators had access to components in the production CDE and that this access matched defined job functions. Documentation Reviewed: POL-01 Data Security Policies and Procedures AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
7.1.4 Require documented approval by authorized parties specifying required privileges.			☒	☐	☐	☐	☐
7.1.4 Select a sample of user IDs and compare with documented approvals to verify that: ● Documented approval exists for the assigned privileges. ● The approval was by authorized parties.	**Identify the sample** of user IDs selected for this testing procedure.	Sample Set-3: New Hires A sample of user IDs assigned to new employees were selected and compared with the documented approval within each of the employee's access request forms. All access requests are submitted and inherently approved by the hiring manager. Documentation Reviewed: EMP-00 Employee Roster					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● That specified privileges match the roles assigned to the individual.	For each user ID in the selected sample, **describe how**:						
	● Documented approval exists for the assigned privileges.	360 Advanced inspected user access requests for a sample of new employees to verify that documented approval existed for the assigned privileges. Access requests were documented in the Request Tracker ticketing system using pre-defined new hire configuration items in addition to being documented within a new hire checklist form for all access requests to systems within the CDE. Documentation Reviewed: SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing)					
	● The approval was by authorized parties.	360 Advanced inspected user access requests for a sample of new employees to verify that documented approval was by authorized parties. Access requests were documented and approved by the hiring manager within the Request Tracker ticketing system using pre-defined new hire configuration items in addition to being documented within a new hire checklist form for all access requests to systems within the CDE. Documentation Reviewed: SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing)					
	● That specified privileges match the roles assigned to the individual.	360 Advanced inspected user quarterly access review for the users sampled and compared them with user access configurations within system components to verify that specified privileges matched the roles assigned to the individual. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:							
7.2 Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows:							
7.2.1 Coverage of all system components.			☒	☐	☐	☐	☐
7.2.1 Confirm that access control systems are in place on all system components.	**Identify vendor documentation** examined.	Center for Internet Security - https://benchmarks.cisecurity.org CIS Microsoft Windows Server 2016 Benchmark CIS Microsoft Windows Server 2019 Benchmark CIS Microsoft SQL Server 2017 Benchmark CIS Benchmarks for Amazon Web Services Foundations SVN Access Manager Documentation - http://svn-access-mana.sourceforge.net					
	Describe how system settings and the vendor documentation verified that access control systems are in place on all system components.	360 Advanced inspected system settings and vendor documentation to verify that access control systems were in place on all system components. Configuration settings were compared to vendor documentation to ensure proper implementation of access control within all system components. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
7.2.2 Assignment of privileges to individuals based on job classification and function.			☒	☐	☐	☐	☐
7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	**Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	360 Advanced inspected system settings and vendor documentation to verify that access control systems were configured to enforce privileges assigned to individuals based on job classification and function. Assignment of privileges was accomplished by adding individuals to predefined groups that were assigned system permissions based on job classification and function. In addition, configuration settings were compared to vendor documentation to ensure proper implementation of access control within all system components. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions					
7.2.3 Default "deny-all" setting.			☒	☐	☐	☐	☐
7.2.3 Confirm that the access control systems have a default "deny-all" setting.	**Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems have a default "deny-all" setting.	360 Advanced inspected system settings and vendor documentation to verify that access control systems had a default "deny-all" setting. The systems in scope used discretionary access controls which, by default, denies all access unless explicitly permitted. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
7.3 Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are: ● Documented, ● In use, and ● Known to all affected parties.	**Identify the document reviewed to** verify that security policies and operational procedures for restricting access to cardholder data are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for restricting access to cardholder data are: ● In use ● Known to all affected parties	Nadine Chahal - General Counsel					

Requirement 8: Identify and authenticate access to system components

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:			☒	☐	☐	☐	☐
8.1.a Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8.	**Identify the written procedures for user identification management** examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8: ● Assign all users a unique ID before allowing them to access system components or cardholder data. ● Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. ● Immediately revoke access for any terminated users. ● Remove/disable inactive user accounts at least every 90 days. ● Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: ● Enabled only during the time period needed and disabled when not in use. ● Monitored when in use. ● Limit repeated access attempts by locking out the user ID after not more than six attempts. ● Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. ● If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	POL-01 Data Security Policies and Procedures				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.b Verify that procedures are implemented for user identification management, by performing the following:							
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.			☒	☐	☐	☐	☐
8.1.1 Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data.	**Identify the responsible administrative personnel** interviewed who confirm that all users are assigned a unique ID for access to system components or cardholder data.	Alex Umansky - Senior Software Engineer					
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.			☒	☐	☐	☐	☐
8.1.2 For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.	**Identify the sample** of privileged user IDs selected for this testing procedure.	User listings and permissions were inspected for each sampled system components to verify that accounts with privileged access were assigned only to individuals necessary for their job function and restricted to privileges necessary to perform their duties. Sample of Users with Privileged Access: Alexander Umansky Chris Bosner					
	Identify the sample of general user IDs selected for this testing procedure.	Not Applicable. Fairfax did not have any general users with access to system components within the CDE.					
	Describe how observed system settings and the associated authorizations verified that each ID has been implemented with only the privileges specified on the documented approval:						
	• For the sample of privileged user IDs.	360 Advanced inspected access request tickets and user access configurations for a sample of system components to verify that permissions were configured as appropriate for the privileged user role as documented within policies. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions					
	• For the sample of general user IDs.	Not Applicable. Fairfax did not have any general users with access to system components within the CDE.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.3 Immediately revoke access for any terminated users.			☒	☐	☐	☐	☐
8.1.3.a Select a sample of users terminated in the past six months, and review current user access lists—for both local and remote access—to verify that their IDs have been deactivated or removed from the access lists.	**Identify the sample** of users terminated in the past six months that were selected for this testing procedure.	Sample Set-5: Terminated Employees NOTE: These users had no access to the production environment. However, termination procedures followed the same processes across the organization whether it be a privileged user or non-privileged user. These procedures were validated to ensure compliance with this requirement.					
	Describe how the current user access lists for ***local access*** verified that the sampled user IDs have been deactivated or removed from the access lists.	360 Advanced inspected user access configurations to verify that the sampled user IDs had been deactivated or removed from access lists that allow local access. A comparison of terminated employees to user access lists for local access to system components was performed and no exceptions found. In addition, quarterly access reviews are performed by comparing employee rosters with current system user listings. Documentation Reviewed: RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions					
	Describe how the current user access lists for ***remote access*** verified that the sampled user IDs have been deactivated or removed from the access lists.	360 Advanced inspected user access configurations to verify that the sampled user IDs had been deactivated or removed from access lists that allow remote access. A comparison of terminated employees to user access lists for local access to system components was performed and no exceptions found. In addition, quarterly access reviews are performed by comparing employee rosters with current system user listings to ensure correct membership for groups assigned with privileged rights. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions EMP-03.1 Terminated Employee Access Removal Records RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions VPN-01 VPN Client User Listing					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.3.b Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated.	*For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination.	360 Advanced inspected the terminated user checklist to verify that the list was comprehensive and included the removal for physical and logical authentication methods in use. 360 Advanced noted that no physical MFA tokens were assigned to gain access to the CDE located within the AWS environment. Only Google Authenticator soft tokens were used in conjunction with OpenVPN credentials to gain remote VPN access to the CDE. Removal of these credentials were included within the termination checklist form. In addition, quarterly access reviews are performed by comparing employee rosters with current system user listings to ensure all terminated employees have been disabled or removed. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions EMP-03.1 Terminated Employee Access Removal Records RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions VPN-01 VPN Client User Listing					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated.	360 Advanced inspected the terminated user checklist for a sample of terminated employees to verify that the list was comprehensive and included the removal for physical and logical authentication methods in use. Procedures for completing the process were demonstrated during the interview and the form ensured that physical authentication methods would be verified and returned/deactivated if the access was applicable for the terminated employee. 360 Advanced noted that no physical keys were assigned to gain access to the CDE located within the AWS environment. In addition, quarterly access reviews are performed by comparing employee rosters with current system user listings to ensure all terminated employees have been disabled or removed. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions EMP-03.1 Terminated Employee Access Removal Records RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions VPN-01 VPN Client User Listing					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.4 Remove/disable inactive user accounts within 90 days.			☒	☐	☐	☐	☐
8.1.4 Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	**Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled.	360 Advanced inspected user access configurations and a quarterly access review tickets to verify that inactive accounts over 90 days were disabled or removed. Administrators manually reviewed system access configurations and disabled or removed accounts that have been inactive for over 90 days. User access configurations indicated no instances of accounts that were inactive for over 90 days. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions EMP-03.1 Terminated Employee Access Removal Records RVW-03.1 Review of Logical Access for Privileged Users SRV-01.1 Server User Listing & Access Permissions VPN-01 VPN Client User Listing					
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: ● Enabled only during the time period needed and disabled when not in use. ● Monitored when in use.			☐	☐	☒	☐	☐
8.1.5.a Interview personnel and observe processes for managing accounts used by third parties to access, support, or maintain system components to verify that accounts used for remote access are: ● Disabled when not in use. ● Enabled only when needed by the third party, and disabled when not in use.	**Identify the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are: ● Disabled when not in use. ● Enabled only when needed by the third party, and disabled when not in use.	Not Applicable. Fairfax did not have vendors who accessed system components within the CDE.					
	Describe how processes for managing third party accounts were observed to verify that accounts used for remote access are:						
	● Disabled when not in use.	Not Applicable. Fairfax did not have vendors who accessed system components within the CDE.					
	● Enabled only when needed by the third party, and disabled when not in use.	Not Applicable. Fairfax did not have vendors who accessed system components within the CDE.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.5.b Interview personnel and observe processes to verify that third party remote access accounts are monitored while being used.	**Identify the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are monitored while being used.	Not Applicable. Fairfax did not have vendors who accessed system components within the CDE.					
	Describe how processes for managing third party remote access were observed to verify that accounts are monitored while being used.	Not Applicable. Fairfax did not have vendors who accessed system components within the CDE.					
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.			☒	☐	☐	☐	☐
8.1.6.a For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	For each item in the sample, **describe how** system configuration settings verified that authentication parameters are set to require that user accounts be locked after not more than six invalid logon attempts.	360 Advanced inspected account lockout policies configured for the sample of system components to verify that authentication parameters were set to lock out user accounts after no more than six invalid logon attempts. User accounts to system components were Active Directory integrated and configured to be locked out after five failed logon attempts. AWS IAM is used for administrative access to the Amazon cloud services and does not support account lockout policies. However, multi-factor authentication is used for user accounts that are registered for administrative access. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA AWS-02 AWS IAM - Password Policy SRV-01.2 Server Password & Account Lockout SRV-02 Server Hardening Scripts & Security Enforcement					
8.1.6.b ***Additional procedure for service provider assessments only:*** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	*Additional procedure for service provider assessments only,* **identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
	Describe how implemented processes were observed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.			☒	☐	☐	☐	☐
8.1.7 For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	For each item in the sample, **describe how** system configuration settings verified that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	360 Advanced inspected account lockout policies configured for the sample of system components to verify that authentication parameters were set to lock out user accounts for a minimum of 30 minutes. User accounts to system components were Active Directory integrated and configured to be locked out for a duration of 30 minutes. AWS IAM is used for administrative access to the Amazon cloud services and does not support account lockout policies. However, multi-factor authentication is used for user accounts that are registered for administrative access. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA AWS-02 AWS IAM - Password Policy SRV-01.2 Server Password & Account Lockout SRV-02 Server Hardening Scripts & Security Enforcement					
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.			☒	☐	☐	☐	☐
8.1.8 For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	For each item in the sample, **describe how** system configuration settings verified that system/session idle time out features have been set to 15 minutes or less.	360 Advanced inspected session timeout values for the sample of system components to verify that system/session idle time out features were configured to 15 minutes or less. Remote management settings were configured to disconnect and require re-authentication for sessions that were idle for 15 minutes. In addition, system components were managed through jump servers which were configured to disconnect remote session after 15 minutes of inactivity. Workstations located within the secure data processing room at the Tampa office were configured with screen saver settings that enforced a timeout after 15 minutes of inactivity. Documentation Reviewed: PC-04 PC Screen Saver Settings SRV-01.6 Server Remote Management & Idle Timeouts SRV-02 Server Hardening Scripts & Security Enforcement					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: ● Something you know, such as a password or passphrase. ● Something you have, such as a token device or smart card. ● Something you are, such as a biometric.			☒	☐	☐	☐	☐
8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following: ● Examine documentation describing the authentication method(s) used. ● For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	**Identify the document** describing the authentication method(s) used that was reviewed to verify that the methods require users to be authenticated using a unique ID and additional authentication for access to the cardholder data environment.	POL-01 Data Security Policies and Procedures					
	Describe the authentication methods used (for example, a password or passphrase, a token device or smart card, a biometric, etc.) for each type of system component.	360 Advanced observed the following authentication methods for each type of system component: AWS Access: Unique ID / Password with MFA Google Authenticator soft token RDP Access: Unique ID / Password (established after VPN) VPN Client Access: Unique ID / Password with MFA Google Authenticator soft token					
	For each type of authentication method used and for each type of system component, **describe how** the authentication method was observed to be functioning consistently with the documented authentication method(s).	360 Advanced observed system administrators log on to the sample of system components and inspected access control policies to verify that the authentication method observed were consistent with documented procedures.					
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.			☒	☐	☐	☐	☐
8.2.1.a Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage.	**Identify the vendor documentation** examined to verify that passwords are protected with strong cryptography during transmission and storage.	Center for Internet Security - https://benchmarks.cisecurity.org CIS Microsoft Windows Server 2016 Benchmark CIS Microsoft Windows Server 2019 Benchmark CIS Microsoft SQL Server 2017 Benchmark CIS Benchmarks for Amazon Web Services Foundations					
	Identify the sample of system components selected for this testing procedure.	Sample Set-1: Servers					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	For each item in the sample, **describe how** system configuration settings verified that passwords are protected with strong cryptography during ***transmission***.	360 Advanced inspected system configurations to verify that passwords were transmitted using strong cryptography as defined by vendor documentation and industry hardening guides. ● AWS Management Console: TLS v1.2 ● Windows Servers: RDP (High) for remote sessions and Kerberos (AES-256-CTS-HMAC-SHA1-96) for network connections ● VPN Client Access: TLS v1.2 with Google Authenticator MFA ● Fairfax Quick Modules: TLS v1.2 Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data SRV-01.3 Server Running Services & Listening Ports SRV-01.6 Server Remote Management & Idle Timeouts VPN-02 VPN Client Authentication & Encryption					
	For each item in the sample, **describe how** system configuration settings verified that passwords are protected with strong cryptography during ***storage***.	360 Advanced inspected system configurations to verify that passwords were stored using strong cryptography as defined by vendor documentation and industry hardening guides. ● AWS Management Console: Responsibility of Amazon ● Windows Servers: NT MD4 hash ● SQL Database Servers: Integrated with Windows Active Directory ● VPN Client Access: Integrated with Windows Active Directory ● Fairfax Quick Pay: Integrated with Windows Active Directory Documentation Reviewed: APP-01.4 Application Configuration - Encrypt Storage of Sensitive Data Passwords Technical Overview - https://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.1.b For a sample of system components, examine password files to verify that passwords are unreadable during storage.	*For each item in the sample at 8.2.1.a,* **describe how** password files verified that passwords are unreadable during storage.	360 Advanced observed password files for a sample of selected components to verify that passwords were rendered unreadable during storage. ● AWS Management Console: Responsibility of Amazon ● Windows Servers: NT MD4 hash ● SQL Database Servers: Integrated with Windows Active Directory ● VPN Client Access: Integrated with Windows Active Directory ● Fairfax Quick Pay: Integrated with Windows Active Directory Documentation Reviewed: APP-01.4 Application Configuration - Encrypt Storage of Sensitive Data SRV-01.2 Server Password & Account Lockout Passwords Technical Overview - https://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx					
8.2.1.c For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission.	*For each item in the sample at 8.2.1.a,* **describe how** password files verified that passwords are unreadable during transmission.	360 Advanced inspected system configurations to verify that passwords were transmitted using strong cryptography as defined by vendor documentation and industry hardening guides. ● AWS Management Console: TLS v1.2 ● Windows Servers: RDP (High) for remote sessions and Kerberos (AES-256-CTS-HMAC-SHA1-96) for network connections ● VPN Client Access: Active Directory/LDAP Integrated with Google Authenticator MFA ● Fairfax Quick Modules: TLS v1.2 Documentation Reviewed: APP-01.3 Application - Encrypt Transmission of Sensitive Data MFA-01 MFA Login from Internal & External Networks SRV-01.3 Server Running Services & Listening Ports SRV-01.6 Server Remote Management & Idle Timeouts VPN-02 VPN Client Authentication & Encryption					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.1.d ***Additional procedure for service provider assessments only:*** Observe password files to verify that non-consumer customer passwords are unreadable during storage.	*Additional procedure for service provider assessments only: for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during storage.	Not Applicable. Fairfax did not maintain non-consumer customer passwords with access to the CDE.					
8.2.1.e ***Additional procedure for service provider assessments only:*** Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission.	*Additional procedure for service provider assessments only: for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during transmission.	Not Applicable. Fairfax did not maintain non-consumer customer passwords with access to the CDE.					
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.			☒	☐	☐	☐	☐
8.2.2 Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the authentication credential is modified.	**Identify the document** examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user's identity is verified before the authentication credential is modified.	POL-01 Data Security Policies and Procedures					
	Describe the non-face-to-face methods used for requesting password resets.	A user requesting a password reset that is not in the physical presence of appropriate and designated IT personnel must undergo a verification process consisting of verbal confirmation of vital statistical information such as date of birth or Social Security number.					
	For each non-face-to-face method, **describe how** security personnel were observed to verify the user's identity before the authentication credential was modified.	360 Advanced noted that there were no password resets during the assessment period. However, personnel described the password reset procedures and explained that users would follow the above process to confirm identity.					
8.2.3 Passwords/passphrases must meet the following: ● Require a minimum length of at least seven characters. ● Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.			☒	☐	☐	☐	☐
8.2.3.a For a sample of system components, inspect system configuration	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity: ● Require a minimum length of at least seven characters. ● Contain both numeric and alphabetic characters.	*For each item in the sample,* **describe how** system configuration settings verified that user password/passphrase parameters are set to require at least the following strength/complexity:						
	● Require a minimum length of at least seven characters.	360 Advanced inspected password policies configured for the sample of system components to verify that user password parameters required a minimum length of at least seven characters. Active Directory group policy was used to enforce these security settings and were applied to all user objects within the domain. AWS IAM is used for administrative access to the Amazon cloud services and was configured to require a minimum password length of eight characters. In addition, multi-factor authentication is used for user accounts that are registered for administrative access. Documentation Reviewed: AWS-02 AWS IAM - Password Policy SRV-01.2 Server Password & Account Lockout SRV-02 Server Hardening Scripts & Security Enforcement					
	● Contain both numeric and alphabetic characters.	360 Advanced inspected password policies configured for the sample of system components to verify that user password parameters required passwords to contain both numeric and alphabetic characters. Active Directory group policy was used to enforce these security settings and were applied to all user objects within the domain. AWS IAM is used for administrative access to the Amazon cloud services and was configured to require at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character. In addition, multi-factor authentication is used for user accounts that are registered for administrative access. Documentation Reviewed: AWS-02 AWS IAM - Password Policy SRV-01.2 Server Password & Account Lockout SRV-02 Server Hardening Scripts & Security Enforcement					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.3.b ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: ● Require a minimum length of at least seven characters. ● Contain both numeric and alphabetic characters.	*Additional procedure for service provider assessments only:* **Identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: ● A minimum length of at least seven characters. ● Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
	Describe how internal processes were observed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:						
	● A minimum length of at least seven characters.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
	● Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
8.2.4 Change user passwords/passphrases at least once every 90 days.			☒	☐	☐	☐	☐
8.2.4.a For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days.	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					
	For each item in the sample, **describe how** system configuration settings verified that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days.	360 Advanced inspected password policies configured for the sample of system components to verify that user password parameters required users to change passwords at least once every 90 days. Active Directory group policy was used to enforce these security settings and were applied to all user objects within the domain. AWS IAM is used for administrative access to the Amazon cloud services and was configured to never expire passwords. However, multi-factor authentication is used for user accounts that are registered for administrative access. Documentation Reviewed: AWS-02 AWS IAM - Password Policy SRV-01.2 Server Password & Account Lockout SRV-02 Server Hardening Scripts & Security Enforcement					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.4.b ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that: ● Non-consumer customer user passwords/passphrases are required to change periodically; and ● Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	*Additional procedure for service provider assessments only*, **identify the documented internal processes and customer/user documentation** reviewed to verify that: ● Non-consumer customer user passwords/passphrases are required to change periodically; and ● Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
	Describe how internal processes were observed to verify that:						
	● Non-consumer customer user passwords/passphrases are required to change periodically; and	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
	● Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.			☒	☐	☐	☐	☐
8.2.5.a For a sample of system components, obtain and inspect system	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
configuration settings to verify that password/passphrases parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	*For each item in the sample,* **describe how** system configuration settings verified that password/passphrase parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	360 Advanced inspected password policies configured for the sample of system components to verify that password parameters required that new passwords cannot be the same as the four previously used passwords. Active Directory group policy was used to enforce these security settings and were applied to all user objects within the domain. AWS IAM is used for administrative access to the Amazon cloud services and was configured to prevent password reuse of up to three of the last previously used passwords. However, multi-factor authentication is used for user accounts that are registered for administrative access. Documentation Reviewed: AWS-02 AWS IAM - Password Policy SRV-01.2 Server Password & Account Lockout SRV-02 Server Hardening Scripts & Security Enforcement					
8.2.5.b *Additional Procedure for service provider assessments only:* Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.	*Additional procedure for service provider assessments only,* **identify the documented internal processes and customer/user documentation** reviewed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					
	Describe how internal processes were observed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.	Not Applicable. Fairfax did not maintain any non-consumer user accounts with access to cardholder data.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.			☒	☐	☐	☐	☐
8.2.6 Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use.	**Identify the documented password procedures** examined to verify the procedures define that: ● First-time passwords/passphrases must be set to a unique value for each user. ● First-time passwords/passphrases must be changed after the first use. ● Reset passwords/passphrases must be set to a unique value for each user. ● Reset passwords/passphrases must be changed after the first use.	POL-01 Data Security Policies and Procedures					
	Describe how security personnel were observed to:						
	● Set first-time passwords/passphrases to a unique value for each new user.	360 Advanced observed a demonstration of the process for generating first-time passwords for new users to verify that a random password generator was used to create a unique value for each user. For Amazon user accounts, the AWS IAM interface supported an option to create or modify an account with a new auto-generated password.					
	● Set first-time passwords/passphrases to be changed after first use.	360 Advanced observed a demonstration of the process for creating new users to verify that first-time passwords were to be changed after first use by setting the flag in Active Directory to require a new password after first use. For Amazon user accounts, the AWS IAM interface supported an option to require users to create a new password at next sign-in.					
	● Set reset passwords/passphrases to a unique value for each existing user.	360 Advanced observed a demonstration of the process for resetting passwords for existing users to verify that a random password generator was used to create a unique value for each user. For Amazon user accounts, the AWS IAM interface supported an option to replace an existing password with a new auto-generated password.					
	● Set reset passwords/passphrases to be changed after first use.	360 Advanced observed a demonstration of the process for resetting passwords for existing users to verify that passwords were to be changed after first use by setting the flag in Active Directory to require a new password after first use. For Amazon user accounts, the AWS IAM interface supported an option to require users to create a new password at next sign-in.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*							
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.			☒	☐	☐	☐	☐
8.3.1.a Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE.	**Identify the sample of network and/or system components** examined for this testing procedure.	OpenVPN PRD1: SSL VPN (AWS Marketplace / Appliance)					
	Describe how the configurations verify that multi-factor authentication is required for all non-console access into the CDE.	360 Advanced inspected VPN client configurations to verify that multi-factor authentication was required for all remote access by personnel. Remote access inside and outside the AWS cloud environment required the use of an SSL VPN with MFA enabled using Google Authenticator. In addition, personnel must access a designated jump server assigned specifically for the management and administration of system components within the CDE environment. Documentation Reviewed: MFA-01 MFA Login from Internal & External Networks SRV-01.1 Server User Listing & Access Permissions VPN-02 VPN Client Authentication & Encryption					
8.3.1.b Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used.	**Identify the sample of administrator personnel** observed logging in to the CDE.	Alex Umansky - Senior Software Engineer					
	Describe the multi-factor authentication methods observed to be in place for a personnel non-console log ins to the CDE.	360 Advanced observed the multi-factor authentication process that provided remote access into the CDE environment. Remote access inside and outside the AWS cloud environment required the use of an SSL VPN with MFA enabled using Google Authenticator. Personnel were then required to access a designated jump server assigned specifically for the management and administration of system components within the CDE environment.					
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.			☒	☐	☐	☐	☐
	Describe how system configurations for remote access servers and systems verified that multi-factor authentication is required for:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.3.2.a Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for: ● All remote access by personnel, both user and administrator, and ● All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes).	● All remote access by personnel, both user and administrator, and	360 Advanced inspected VPN client configurations to verify that multi-factor authentication was required for all remote access by personnel. Remote access inside and outside the AWS cloud environment required the use of an SSL VPN with MFA enabled using Google Authenticator. In addition, personnel must access a designated jump server assigned specifically for the management and administration of system components within the CDE environment. Documentation Reviewed: MFA-01 MFA Login from Internal & External Networks SRV-01.1 Server User Listing & Access Permissions VPN-02 VPN Client Authentication & Encryption					
	● All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes).	Not Applicable. Fairfax did not allow third-party/vendor remote access to in-scope systems or components.					
8.3.2.b Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used.	**Identify the sample of personnel** observed connecting remotely to the network.	Alex Umansky - Senior Software Engineer					
	For each individual in the sample, **describe how** multi-factor authentication was observed to be required for remote access to the network.	360 Advanced observed the multi-factor authentication process that provided remote access into the CDE environment. Remote access inside and outside the AWS cloud environment required the use of an SSL VPN with MFA enabled using Google Authenticator. Personnel were then required to access a designated jump server assigned specifically for the management and administration of system components within the CDE environment.					
8.4 Document and communicate authentication policies and procedures to all users including: ● Guidance on selecting strong authentication credentials. ● Guidance for how users should protect their authentication credentials. ● Instructions not to reuse previously used passwords. ● Instructions to change passwords if there is any suspicion the password could be compromised.			☒	☐	☐	☐	☐
8.4.a Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users.	**Identify the documented policies and procedures** examined to verify authentication procedures define that authentication procedures and policies are distributed to all users.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed who confirm that authentication policies and procedures are distributed to all users.	Nadine Chahal - General Counsel					
8.4.b Review authentication policies and procedures that are distributed to users and verify they include: ● Guidance on selecting strong authentication credentials. ● Guidance for how users should protect their authentication credentials. ● Instructions for users not to reuse previously used passwords. ● Instructions to change passwords if there is any suspicion the password could be compromised.	**Identify the documented authentication policies and procedures** that are distributed to users reviewed to verify they include: ● Guidance on selecting strong authentication credentials. ● Guidance for how users should protect their authentication credentials. ● Instructions for users not to reuse previously used passwords. ● That users should change passwords if there is any suspicion the password could be compromised.	POL-01 Data Security Policies and Procedures					
8.4.c Interview a sample of users to verify that they are familiar with authentication policies and procedures.	**Identify the sample** of users interviewed for this testing procedure.	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
	For each user in the sample, **summarize the relevant details** discussed that verify that they are familiar with authentication policies and procedures.	Personnel described the use and maintenance of all authentication procedures including proper password generation and protection. In addition, annual security awareness training that includes policies was performed to re-enforce the guidance and importance of these authentication procedures. A training acknowledgement is signed by personnel upon completion of the training. Documentation Reviewed: SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing) EMP-02.1 Employee Annual Security Awareness Refresher					
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: ● Generic user IDs are disabled or removed. ● Shared user IDs do not exist for system administration and other critical functions. ● Shared and generic user IDs are not used to administer any system components.			☒	☐	☐	☐	☐
	Identify the sample of system components selected for this testing procedure.	Sample Set-1: Servers					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.5.a For a sample of system components, examine user ID lists to verify the following: ● Generic user IDs are disabled or removed. ● Shared user IDs for system administration activities and other critical functions do not exist. ● Shared and generic user IDs are not used to administer any system components.	*For each item in the sample,* **describe how** the user ID lists verified that:						
	● Generic user IDs are disabled or removed.	360 Advanced inspected user access configurations for the sample of system components to verify that generic user IDs were disabled. Documentation Reviewed: SRV-01.1 Server User Listing & Access Permissions					
	● Shared user IDs for system administration activities and other critical functions do not exist.	360 Advanced inspected user access configurations for the sample of system components to verify that the use of any shared user IDs for system administration or other critical functions did not exist. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
	● Shared and generic user IDs are not used to administer any system components.	360 Advanced inspected user access configurations for the sample of system components to verify that shared and generic user IDs were not used to administer any system components. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA DEV-01 Code Repo & Versioning Tools - User Listing & Permissions DEV-02 Integration & Deployment Tools - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
8.5.b Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.	**Identify the documented policies and procedures** examined to verify authentication policies/procedures define that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.	POL-01 Data Security Policies and Procedures					
8.5.c Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.	**Identify the system administrators** interviewed who confirm that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.	Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*			☐	☐	☒	☐	☐
8.5.1 ***Additional procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer.	**Identify the documented procedures** examined to verify that different authentication credentials are used for access to each customer.	Not Applicable. Fairfax did not require or maintain remote access to customer sites or systems.					
	Identify the responsible personnel interviewed who confirm that different authentication credentials are used for access to each customer	Not Applicable. Fairfax did not require or maintain remote access to customer sites or systems.					
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows: ● Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. ● Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.			☒	☐	☐	☐	☐
8.6.a Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include: ● Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. ● Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.	**Identify the documented authentication policies and procedures** examined to verify the procedures for using authentication mechanisms define that: ● Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. ● Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.	POL-01 Data Security Policies and Procedures					
8.6.b Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts.	**Identify the security personnel** interviewed who confirm that authentication mechanisms are assigned to an account and not shared among multiple accounts.	Alex Umansky - Senior Software Engineer					
8.6.c Examine system configuration settings and/or physical controls, as	**Identify the sample** of system components selected for this testing procedure.	Sample Set-1: Servers					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access.	*For each item in the sample,* **describe how** system configuration settings and/or physical controls, as applicable, verified that controls are implemented to ensure only the intended account can use that mechanism to gain access.	360 Advanced inspected system configuration settings for the sample of system components to verify that controls were implemented to ensure only the intended account can use that mechanism to gain access. User and group listings were compared to system role permissions to ensure only users who are assigned administrative privileges can gain access to the system components they are responsible for. In addition, configurations indicated that MFA was required for all remote access connections using software tokens assigned only for authorized IT administrators. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA MFA-01 MFA Login from Internal & External Networks SRV-01.1 Server User Listing & Access Permissions VPN-02 VPN Client Authentication & Encryption					
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: ● All user access to, user queries of, and user actions on databases are through programmatic methods. ● Only database administrators have the ability to directly access or query databases. ● Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).			☐	☐	☒	☐	☐
8.7.a Review database and application configuration settings and verify that all users are authenticated prior to access.	**Identify** all databases containing cardholder data.	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					
	Describe how database and/or application configuration settings verified that all users are authenticated prior to access.	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.7.b Examine database and application configuration settings to verify that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).	*For each database from 8.7.a,* **describe how** the database and application configuration settings verified that all user access to, user queries of, and user actions on the database are through programmatic methods only.	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					
8.7.c Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators.	*For each database from 8.7.a*, **describe how** database application configuration settings verified that user direct access to or queries of databases are restricted to database administrators.	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					
8.7.d Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).	*For each database from 8.7.a:*						
	● Identify applications with access to the database.	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					
	● Describe how database access control settings, database application configuration settings and related application IDs verified that application IDs can only be used by the applications.	Not Applicable. The Fairfax web interface accepting credit card information utilizes third-party processing payment scripts within iFrames that redirects customer cardholder data and sensitive authentication data to the third-party payment processor for tokenization, storage, and processing. This sensitive data is not stored on Fairfax systems in any form.					
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
8.8 Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are: ● Documented, ● In use, and ● Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for identification and authentication are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for identification and authentication are: ● In use ● Known to all affected parties	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					

Requirement 9: Restrict physical access to cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.			☒	☐	☐	☐	☐
9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. ● Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. ● Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder data environment and verify that they are "locked" to prevent unauthorized use.	**Identify and briefly describe** all of the following with systems in the cardholder data environment:						
	● All computer rooms	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	● All data centers	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	● Any other physical areas	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	For each area identified (add rows as needed), complete the following:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe the physical security controls observed to be in place, including authorized badges and lock and key.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office.					
	Identify the randomly selected systems in the cardholder environment for which a system administrator login attempt was observed.	The Fairfax frontend CDE where potential cardholder data would be scanned included two Windows workstations which hosted the scanning application.					
	Describe how consoles for the randomly selected systems were observed to be "locked" when not in use.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE where potential cardholder data would be scanned included two Windows workstations which hosted the scanning application. These systems were observed to be locked while performing the virtual onsite walkthrough.					
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*			☒	☐	☐	☐	☐
9.1.1.a Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas.	**Describe** either the video cameras or access control mechanisms (or both) observed to monitor the entry/exit points to sensitive areas.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Video cameras were observed to be in place at the entrance of the office and also within the locked data processing room.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.1.1.b Verify that either video cameras or access control mechanisms (or both) are protected from tampering or disabling.	**Describe how** either the video cameras or access control mechanisms (or both) were observed to be protected from tampering and/or disabling.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Video cameras were observed to be out of reach and within tamper-proof casings at the entrance of the office and also within the locked data processing room.					
9.1.1.c Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months.	**Describe how** the data from video cameras and/or access control mechanisms were observed to be reviewed.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Video cameras were observed to be monitored by the front desk receptionist.					
	Describe how data was observed to be stored for at least three months.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Video footage was observed to be retained for at least three months.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*			☒	☐	☐	☐	☐
9.1.2 Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly-accessible network jacks.	**Identify the responsible personnel** interviewed who confirm that physical and/or logical controls are in place to restrict access to publicly accessible network jacks.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Additionally, there are no areas within the office to be considered for public use and all visitors must be escorted at all times.					
	Describe how physical and/or logical controls were observed to be in place to restrict access to publicly-accessible network jacks.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Additionally, there are no areas within the office to be considered for public use and all visitors must be escorted at all times.					
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.			☒	☐	☐	☐	☐
9.1.3 Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.	**Describe how** physical access was observed to be restricted to the following:						
	• Wireless access points	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Networking equipment, including wireless access points, are stored in a closet within this room where the ISP demarc resides.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Wireless gateways	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Networking equipment, including wireless access points, are stored in a closet within this room where the ISP demarc resides. However, there are no wireless gateways that are in scope of this assessment.					
	• Wireless handheld devices	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Networking equipment, including wireless access points, are stored in a closet within this room where the ISP demarc resides. However, there are no wireless handheld devices that are in scope of this assessment.					
	• Network/communications hardware	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Networking equipment, including wireless access points, are stored in a closet within this room where the ISP demarc resides.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Telecommunication lines	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Networking equipment, including wireless access points, are stored in a closet within this room where the ISP demarc resides.					
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: ● Identifying onsite personnel and visitors (for example, assigning badges). ● Changes to access requirements. ● Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).			☒	☐	☐	☐	☐
9.2.a Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors. ● Verify procedures include the following: ● Identifying onsite personnel and visitors (for example, assigning badges), ● Changing access requirements, and ● Revoking terminated onsite personnel and expired visitor identification (such as ID badges).	**Identify the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following: ● Identifying onsite personnel and visitors (for example, assigning badges), ● Changing access requirements, and ● Revoking terminated onsite personnel and expired visitor identification (such as ID badges).	POL-01 Data Security Policies and Procedures				
9.2.b Examine identification methods (such as ID badges) and observe processes for identifying and distinguishing between onsite personnel and visitors to verify that: ● Visitors are clearly identified, and	**Identify** the identification methods examined.	Badge access and key fobs. Visitors are not given physical access cards of any kind and must always be escorted by Fairfax personnel. NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					
	Describe how processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● It is easy to distinguish between onsite personnel and visitors.	● Visitors are clearly identified, and	360 Advanced observed that visitors were clearly identified. Temporary badge stickers were clearly labeled with markings indicating "Visitor", visitor's company name, employee responsible and badge expiration date.					
	● It is easy to distinguish between onsite personnel and visitors.	360 Advanced observed that visitors were clearly distinguishable from onsite personnel. Temporary badge stickers were clearly labelled with "Visitor", visitor's name, firm represented, and badge issue and expiration date printed on the front. Visitors are not given physical token badges of any kind and must always be escorted by Fairfax personnel.					
9.2.c Verify that access to the identification process (such as a badge system) is limited to authorized personnel.	**Describe how** access to the identification process was observed to be limited to authorized personnel.	360 Advanced observed that access to the data processing room was restricted to key personnel and that issuance of keys to the locked cabinet and safe storing scanned materials were documented through a key control register and sign out sheet.					
9.3 Control physical access for onsite personnel to sensitive areas as follows: ● Access must be authorized and based on individual job function. ● Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.			☒	☐	☐	☐	☐
9.3.a For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that: ● Access to the sensitive area is authorized. ● Access is required for the individual's job function.	**Identify the sample** of onsite personnel with physical access to sensitive areas that were interviewed for this testing procedure.	Robert Castello - Director of Support Services NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					
	For the interview, **summarize the relevant details** discussed to verify that:						
	● Access to the sensitive area is authorized.	360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log with reviews performed on a quarterly basis. Documentation Reviewed: PHY-01 List of Users with Key & Badge Access to Sensitive Areas					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Access is required for the individual's job function.	360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log with reviews performed on a quarterly basis. The access tracking logs contained only personnel who required access per their job function. Documentation Reviewed: PHY-01 List of Users with Key & Badge Access to Sensitive Areas					
9.3.b Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access.	**Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access.	360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log with reviews performed on a quarterly basis. The access tracking logs contained only personnel who required access per their job function. Documentation Reviewed: PHY-01 List of Users with Key & Badge Access to Sensitive Areas					
9.3.c Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas.	**Identify the sample** of users recently terminated.	Sample Set-5: Terminated Employees NOTE: These users had no access to the production environment. However, termination procedures followed the same processes across the organization whether it be a privileged user or non-privileged user. These procedures were validated to ensure compliance with this requirement.					
	For all items in the sample, **provide the name of the assessor** who attests that the access control lists were reviewed to verify the personnel do not have physical access to sensitive areas.	Phillip Hagan, QSA# 204-876					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:							
9.4 Verify that visitor authorization and access controls are in place as follows:							
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.			☒	☐	☐	☐	☐
9.4.1.a Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.	**Identify the documented procedures** examined to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.	Robert Castello - Director of Support Services					
9.4.1.b Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained.	**Describe how** the use of visitor badges or other identification was observed to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained.	360 Advanced observed that visitors were clearly distinguishable from onsite personnel. Temporary badge stickers were clearly labelled with "Visitor", visitor's name, firm represented, and badge issue and expiration date printed on the front. Visitors are not given physical token badges of any kind and must always be escorted by Fairfax personnel. NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.			☒	☐	☐	☐	☐
9.4.2.a Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel.	**Describe how** people within the facility were observed to use visitor badges or other identification.	360 Advanced observed that visitors were clearly distinguishable from onsite personnel. Temporary badge stickers were clearly labelled with "Visitor", visitor's name, firm represented, and badge issue and expiration date printed on the front. Visitors are not given physical token badges of any kind and must always be escorted by Fairfax personnel. NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how visitors within the facility were observed to be easily distinguishable from onsite personnel.	360 Advanced observed that visitors were clearly distinguishable from onsite personnel. Temporary badge stickers were clearly labelled with "Visitor", visitor's name, firm represented, and badge issue and expiration date printed on the front. Visitors are not given physical token badges of any kind and must always be escorted by Fairfax personnel. NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					
9.4.2.b Verify that visitor badges or other identification expire.	**Describe how** visitor badges or other identification were verified to expire.	360 Advanced observed that visitors were clearly distinguishable from onsite personnel. Temporary badge stickers were clearly labelled with "Visitor", visitor's name, firm represented, and badge issue and expiration date printed on the front. Visitors are not given physical token badges of any kind and must always be escorted by Fairfax personnel. NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.			☒	☐	☐	☐	☐
9.4.3 Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration.	**Describe how** visitors leaving the facility were observed to verify they are asked to surrender their badge or other identification upon departure or expiration.	360 Advanced observed that visitors were clearly distinguishable from onsite personnel. Temporary badge stickers were clearly labelled with "Visitor", visitor's name, firm represented, and badge issue and expiration date printed on the front. Visitors are not given physical token badges of any kind and must always be escorted by Fairfax personnel. NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.			☒	☐	☐	☐	☐
	Describe how it was observed that a visitor log is in use to record physical access to:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.4.4.a Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.	• The facility.	360 Advanced observed that a visitor log was in use to record physical access to the facility. Visitors are required to enter their full name, the date and time in, the firm represented, and the reason for visit. NOTE: The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment.					
	• Computer rooms and data centers where cardholder data is stored or transmitted.	360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log. The access tracking logs contained only personnel who required access per their job function. Documentation Reviewed: PHY-01 List of Users with Key & Badge Access to Sensitive Areas					
9.4.4.b Verify that the log contains: • The visitor's name, • The firm represented, and • The onsite personnel authorizing physical access.	**Provide the name of the assessor** who attests that the visitor log contains: • The visitor's name, • The firm represented, and • The onsite personnel authorizing physical access.	Phillip Hagan, QSA# 204-876					
9.4.4.c Verify that the log is retained for at least three months.	**Describe how** visitor logs were observed to be retained for at least three months.	360 Advanced observed visitor logs entries to verify that the logs were retained for at least three months. Binders containing the signed visitor entries were physically filed and archived and kept indefinitely.					
9.5 Physically secure all media.			☒	☐	☐	☐	☐
9.5 Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).	**Identify the documented procedures for protecting cardholder data** reviewed to verify controls for physically securing all media are defined.	Fairfax does not store CHD or any PCI-related data onto portable or backup media outside of Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in its own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. In addition, Fairfax prohibits printing of customer data onto hard-copy materials.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.			☒	☐	☐	☐	☐
9.5.1. Verify that the storage location security is reviewed at least annually to confirm that backup media storage is secure.	**Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Two workstations are used to scan physical hardcopy materials through character recognition engines with the resulting data and images transmitted directly to the backend systems residing in AWS. Fairfax prevents storage of this data onto removable media by disabling USB storage access at the registry level. Documentation Reviewed: MED-01 Electronic Media Encryption & Restriction					
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:			☒	☐	☐	☐	☐
9.6 Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.	**Identify the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. In addition, a locked filing cabinet and safe are used to store documents before and after processing. 360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log. The access tracking logs contained only personnel who required access per their job function.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.6.1 Classify media so the sensitivity of the data can be determined.			☒	☐	☐	☐	☐
9.6.1 Verify that all media is classified so the sensitivity of the data can be determined.	**Describe how** media was observed to be classified so the sensitivity of the data can be determined.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. In addition, a locked filing cabinet and safe are used to store documents before and after processing. All material and electronic equipment stored within the data processing room were designated to be confidential.					
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.			☒	☐	☐	☐	☐
9.6.2.a Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.	**Identify the responsible personnel** interviewed who confirm that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.	Nadine Chahal - General Counsel					
	Identify the records examined for this testing procedure.	PHY-01 List of Users with Key & Badge Access to Sensitive Areas PHY-02 Administrator Listing to Badge Access System					
	Describe how the offsite tracking records verified that all media is logged and sent via secured courier or other delivery method that can be tracked.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. In addition, a locked filing cabinet and safe are used to store documents before and after processing. 360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log. The access tracking logs contained only personnel who required access per their job function.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.6.2.b Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented.	**Identify the sample** of recent offsite tracking logs for all media selected.	PHY-01 List of Users with Key & Badge Access to Sensitive Areas PHY-02 Administrator Listing to Badge Access System					
	For each item in the sample, **describe how** tracking details were observed to be documented.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. In addition, a locked filing cabinet and safe are used to store documents before and after processing. 360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log. The access tracking logs contained only personnel who required access per their job function.					
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).			☒	☐	☐	☐	☐
9.6.3 Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization	**Identify the responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals).	Nadine Chahal - General Counsel					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
is obtained whenever media is moved from a secured area (including when media is distributed to individuals).	*For each item in the sample in 9.6.2.b,* **describe how** proper management authorization was observed to be obtained whenever media is moved from a secured area (including when media is distributed to individuals).	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. In addition, a locked filing cabinet and safe are used to store documents before and after processing. 360 Advanced observed that access to the data processing room was restricted to key personnel specifically only those authorized and required for the individual's job function. The key fob system supports assignable areas based on the individual's position and responsibilities. Additionally, keys to the locked cabinet and safe storing scanned materials were also controlled through a remittance tracking log. The access tracking logs contained only personnel who required access per their job function.					
9.7 Maintain strict control over the storage and accessibility of media.			☒	☐	☐	☐	☐
9.7 Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.	**Identify the documented policy for controlling storage and maintenance of all media** that was reviewed to verify that the policy defines required periodic media inventories.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.			☒	☐	☐	☐	☐
9.7.1 Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually.	**Identify the media inventories logs** reviewed.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Two workstations are used to scan physical hardcopy materials through character recognition engines with the resulting data and images transmitted directly to the backend systems residing in AWS. Fairfax prevents storage of this data onto removable media by disabling USB storage access at the registry level. Because of this, no inventory logs for electronic media was deemed necessary. However, 360 Advanced observed inventory logs of the hard-copy materials used for the scanning process. Documentation Reviewed: MED-01 Electronic Media Encryption & Restriction					
	Describe how the media inventory logs verified that:						
	• Media inventory logs of all media were observed to be maintained.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Two workstations are used to scan physical hardcopy materials through character recognition engines with the resulting data and images transmitted directly to the backend systems residing in AWS. Fairfax prevents storage of this data onto removable media by disabling USB storage access at the registry level. Because of this, no inventory logs for electronic media was deemed necessary. However, 360 Advanced observed inventory logs of the hard-copy materials used for the scanning process. Documentation Reviewed: MED-01 Electronic Media Encryption & Restriction					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Media inventories are performed at least annually.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Two workstations are used to scan physical hardcopy materials through character recognition engines with the resulting data and images transmitted directly to the backend systems residing in AWS. Fairfax prevents storage of this data onto removable media by disabling USB storage access at the registry level. Because of this, no inventory logs for electronic media was deemed necessary. However, 360 Advanced observed inventory logs of the hard-copy materials used for the scanning process. Documentation Reviewed: MED-01 Electronic Media Encryption & Restriction					
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:			☒	☐	☐	☐	☐
9.8 Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following: ● Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. ● Storage containers used for materials that are to be destroyed must be secured. ● Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	**Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following: ● Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. ● Storage containers used for materials that are to be destroyed must be secured. ● Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.			☒	☐	☐	☐	☐
9.8.1.a Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	**Identify the responsible personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	Nadine Chahal - General Counsel					
	Provide the name of the assessor who attests that the procedures state that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed.	Phillip Hagan, QSA# 204-876					
9.8.1.b Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured.	**Describe how** the storage containers used for materials to be destroyed were verified to be secured.	360 Advanced observed locked storage bins were used to store hard-copy materials scheduled to be destroyed by a third-party. However, 360 Advanced noted that full PAN is currently never printed onto hard-copy material. Documentation Reviewed: MED-03 Hard-copy Material Destruction					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.			☒	☐	☐	☐	☐
9.8.2 Verify that cardholder data on electronic media is rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	**Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Two workstations are used to scan physical hardcopy materials through character recognition engines with the resulting data and images transmitted directly to the backend systems residing in AWS. Fairfax prevents storage of this data onto removable media by disabling USB storage access at the registry level. In the event that the hard drive of the scanner workstation must be replaced, Fairfax would physically destroy the drive instead of repurposing it for additional use. Documentation Reviewed: MED-01 Electronic Media Encryption & Restriction					
	If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify the industry-accepted standards** used.	The Fairfax backend CDE existed solely within the data center managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who included these testing procedures in their own assessment. Fairfax reviews the Attestation of Compliance for AWS on an annual basis to ensure that compliance is maintained for this requirement. The Fairfax frontend CDE, where potential cardholder data would be scanned, is hosted within a locked data processing room located at the Tampa office. Two workstations are used to scan physical hardcopy materials through character recognition engines with the resulting data and images transmitted directly to the backend systems residing in AWS. Fairfax prevents storage of this data onto removable media by disabling USB storage access at the registry level. In the event that the hard drive of the scanner workstation must be replaced, Fairfax would physically destroy the drive instead of repurposing it for additional use. Documentation Reviewed: MED-01 Electronic Media Encryption & Restriction					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note:*** *These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*			☐	☐	☒	☐	☐
9.9 Examine documented policies and procedures to verify they include: ● Maintaining a list of devices. ● Periodically inspecting devices to look for tampering or substitution. ● Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices.	**Identify the documented policies and procedures** examined to verify they include: ● Maintaining a list of devices. ● Periodically inspecting devices to look for tampering or substitution. ● Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
9.9.1 Maintain an up-to-date list of devices. The list should include the following: ● Make, model of device. ● Location of device (for example, the address of the site or facility where the device is located). ● Device serial number or other method of unique identification.			☐	☐	☒	☐	☐
9.9.1.a Examine the list of devices to verify it includes: ● Make, model of device. ● Location of device (for example, the address of the site or facility where the device is located). ● Device serial number or other method of unique identification.	**Identify the documented up-to-date list of devices** examined to verify it includes: ● Make, model of device. ● Location of device (for example, the address of the site or facility where the device is located). ● Device serial number or other method of unique identification.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
9.9.1.b Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date.	**Identify the sample** of devices from the list selected for this testing procedure.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
	For all items in the sample, **describe how** the devices and device locations were observed to verify that the list is accurate and up-to-date.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.9.1.c Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc.	**Identify the responsible personnel** interviewed who confirm the list of devices is updated when devices are added, relocated, decommissioned, etc.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*			☐	☐	☒	☐	☐
9.9.2.a Examine documented procedures to verify processes are defined to include the following: ● Procedures for inspecting devices. ● Frequency of inspections.	**Identify the documented procedures** examined to verify that processes are defined to include the following: ● Procedures for inspecting devices. ● Frequency of inspections.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
9.9.2.b Interview responsible personnel and observe inspection processes to verify: ● Personnel are aware of procedures for inspecting devices. ● All devices are periodically inspected for evidence of tampering and substitution.	**Identify the responsible personnel** interviewed who confirm that: ● Personnel are aware of procedures for inspecting devices. ● All devices are periodically inspected for evidence of tampering and substitution.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
	Describe how inspection processes were observed to verify that:						
	● All devices are periodically inspected for evidence of tampering.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
	● All devices are periodically inspected for evidence of substitution.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: ● Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. ● Do not install, replace, or return devices without verification. ● Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). ● Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).			☐	☐	☒	☐	☐
9.9.3.a Review training materials for personnel at point-of-sale locations to verify it includes training in the following: ● Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. ● Not to install, replace, or return devices without verification. ● Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). ● Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	**Identify the training materials for personnel at point-of-sale locations** that were reviewed to verify the materials include training in the following: ● Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. ● Not to install, replace, or return devices without verification. ● Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). ● Reporting all suspicious behavior to appropriate personnel (for example, a manager or security officer). ● Reporting tampering or substitution of devices.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.				
9.9.3.b Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following:	**Identify the sample** of personnel at point-of-sale locations interviewed.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
	For the interview, **summarize the relevant details** discussed that verify interviewees have received training and are aware of the procedures for the following:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Not to install, replace, or return devices without verification. • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
	• Not to install, replace, or return devices without verification.	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
	• Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
	• Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Not Applicable. Fairfax does not support or manage devices that capture payment card data via direct physical interaction.					
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
9.10 Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are: • Documented, • In use, and • Known to all affected parties.	**Identify the document reviewed to** verify that security policies and operational procedures for restricting physical access to cardholder data are documented.	POL-01 Data Security Policies and Procedures PRV-00 Privacy Policy					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for restricting physical access to cardholder data are: • In use • Known to all affected parties	Nadine Chahal - General Counsel					

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.1 Implement audit trails to link all access to system components to each individual user.			☒	☐	☐	☐	☐
10.1 Verify, through observation and interviewing the system administrator, that: ● Audit trails are enabled and active for system components. ● Access to system components is linked to individual users.	**Identify the system administrator(s)** interviewed who confirm that: ● Audit trails are enabled and active for system components. ● Access to system components is linked to individual users.	Alex Umansky - Senior Software Engineer					
	Describe how audit trails were observed to verify the following:						
	● Audit trails are enabled and active for system components.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that audit trails were enabled and active. Documentation Reviewed: AWS-08 AWS CloudTrail Configuration & Logs AWS-09 AWS CloudWatch Configuration & Logs LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
	● Access to system components is linked to individual users.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that access to system components were linked to individual user accounts to provide traceable audit trails in the event an incident occurs. Documentation Reviewed: AWS-08 AWS CloudTrail Configuration & Logs AWS-09 AWS CloudWatch Configuration & Logs LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2 Implement automated audit trails for all system components to reconstruct the following events:			☒	☐	☐	☐	☐
10.2 Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	**Identify the responsible personnel** interviewed who confirm the following from 10.2.1-10.2.7 are logged: ● All individual access to cardholder data. ● All actions taken by any individual with root or administrative privileges. ● Access to all audit trails. ● Invalid logical access attempts. ● Use of and changes to identification and authentication mechanisms, including: - All elevation of privileges. - All changes, additions, or deletions to any account with root or administrative privileges. ● Initialization of audit logs. ● Stopping or pausing of audit logs. ● Creation and deletion of system level objects.	Alex Umansky - Senior Software Engineer					
	Identify the sample of audit logs selected for 10.2.1-10.2.7.	AWS-08 AWS CloudTrail Configuration & Logs AWS-09 AWS CloudWatch Configuration & Logs LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples						
10.2.1 All individual user accesses to cardholder data.			☒	☐	☐	☐	☐
10.2.1 Verify all individual access to cardholder data is logged.	*For all items in the sample at 10.2,* **describe how** configuration settings verified that all individual access to cardholder data is logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax logged access attempts from all in-scope system components. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2.2 All actions taken by any individual with root or administrative privileges.			☒	☐	☐	☐	☐
10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged.	*For all items in the sample at 10.2, describe how configuration settings verified all actions taken by any individual with root or administrative privileges are logged.*	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log all administrative actions on systems in the CDE. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.2.3 Access to all audit trails.			☒	☐	☐	☐	☐
10.2.3 Verify access to all audit trails is logged.	*For all items in the sample at 10.2*, **describe how** configuration settings verified that access to all audit trails is logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax logged access to audit trails on systems in the CDE. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.2.4 Invalid logical access attempts.			☒	☐	☐	☐	☐
10.2.4 Verify invalid logical access attempts are logged.	*For all items in the sample at 10.2,* **describe how** configuration settings verified that invalid logical access attempts are logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log failed access attempts to systems in the CDE. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.			☒	☐	☐	☐	☐
10.2.5.a Verify use of identification and authentication mechanisms is logged.	*For all items in the sample at 10.2,* **describe how** configuration settings verified that use of identification and authentication mechanisms is logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log the use of the identification and authentication mechanisms. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.2.5.b Verify all elevation of privileges is logged.	*For all items in the sample at 10.2,* **describe how** configuration settings verified that all elevation of privileges is logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log elevation of privileges. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	*For all items in the sample at 10.2,* **describe how** configuration settings verified that all changes, additions, or deletions to any account with root or administrative privileges are logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log changes, additions, or deletions to any administrative accounts. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2.6 Initialization, stopping, or pausing of the audit logs.			☒	☐	☐	☐	☐
10.2.6 Verify the following are logged: ● Initialization of audit logs. ● Stopping or pausing of audit logs.	*For all items in the sample at 10.2,* **describe how** configuration settings verified that initialization of audit logs is logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log the initialization of audit logs. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
	For all items in the sample at 10.2, **describe how** configuration settings verified that stopping and pausing of audit logs is logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log any actions to stop or pause audit logs or services. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2.7 Creation and deletion of system-level objects.			☒	☐	☐	☐	☐
10.2.7 Verify creation and deletion of system level objects are logged.	*For all items in the sample at 10.2,* **describe how** configuration settings verified that creation and deletion of system level objects are logged.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that Fairfax configured audit policies to log the creation and deletion of system-level objects. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment. File Integrity Monitoring software was also used to log the modification or deletion of system level objects, specifically system files and configurations. Documentation Reviewed: FIM-01 FIM - Monitored Files & Comparison Schedule					
10.3 Record at least the following audit trail entries for all system components for each event:			☒	☐	☐	☐	☐
10.3 Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	**Identify the responsible personnel** interviewed who confirm that for each auditable event from 10.2.1-10.2.7, the following are included in log entries: ● User identification ● Type of event ● Date and time ● Success or failure indication ● Origination of event	Alex Umansky - Senior Software Engineer					
	Identify the sample of audit logs from 10.2.1-10.2.7 observed to verify the following are included in log entries: ● User identification ● Type of event ● Date and time ● Success or failure indication ● Origination of event	AWS-08 AWS CloudTrail Configuration & Logs AWS-09 AWS CloudWatch Configuration & Logs LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.3.1 User identification			☒	☐	☐	☐	☐
10.3.1 Verify user identification is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that user identification is included in log entries.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that the records included specific user identification. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.3.2 Type of event			☒	☐	☐	☐	☐
10.3.2 Verify type of event is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that type of event is included in log entries.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that the records included the type of event that triggered the log. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.3.3 Date and time			☒	☐	☐	☐	☐
10.3.3 Verify date and time stamp is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that date and time stamp is included in log entries.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that the records included the date and time of the event. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.3.4 Success or failure indication			☒	☐	☐	☐	☐
10.3.4 Verify success or failure indication is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified success or failure indication is included in log entries.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that the records included an indicator for success or failure. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.3.5 Origination of event			☒	☐	☐	☐	☐
10.3.5 Verify origination of event is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified origination of event is included in log entries.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that the records included event origination. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					
10.3.6 Identity or name of affected data, system component, or resource			☒	☐	☐	☐	☐
10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified the identity or name of affected data, system component, or resource is included in log entries.	360 Advanced inspected audit configuration settings and sample log data from local systems, the AlienVault console, and AWS management console (for CloudTrail / CloudWatch logs) to verify that the records included the identification of the affected resource. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*			☒	☐	☐	☐	☐
10.4 Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	**Identify** the time synchronization technologies in use. (If NTP, include version)	NTP version 4					
	Identify the documented time-synchronization configuration standards examined to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	POL-01 Data Security Policies and Procedures					
	Describe how processes were examined to verify that time synchronization technologies are:						
	• Implemented.	360 Advanced inspected time configuration settings and time queries to verify that time synchronization technologies were implemented. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
	• Kept current, per the documented process.	360 Advanced inspected time configuration settings and time queries to verify that time synchronization technologies were implemented. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
10.4.1 Critical systems have the correct and consistent time.			☒	☐	☐	☐	☐
10.4.1.a Examine the process for acquiring, distributing and storing the	**Describe how** the process for acquiring, distributing, and storing the correct time within the organization was examined to verify the following:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
correct time within the organization to verify that: ● Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. ● Where there is more than one designated time server, the time servers peer with one another to keep accurate time. ● Systems receive time information only from designated central time server(s).	● Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	360 Advanced inspected time configuration settings and time queries to verify that only designated time servers received time settings from external sources based on UTC. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
	● Where there is more than one designated time server, the time servers peer with one another to keep accurate time.	360 Advanced inspected time configuration settings and time queries to verify that designated time servers peered with one another to keep consistent and accurate time. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
	● Systems receive time information only from designated central time server(s).	360 Advanced inspected time configuration settings and time queries to verify that systems received time information only from designated central time servers. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify:	**Identify the sample** of system components selected for 10.4.1.b-10.4.2.b	Sample Set-1: Servers					
	For all items in the sample, **describe how** the time-related system-parameter settings verified:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. ● Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. ● Systems receive time only from designated central time server(s).	● Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	360 Advanced inspected time configuration settings and time queries to verify that only designated time servers received time settings from external sources based on UTC. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
	● Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.	360 Advanced inspected time configuration settings and time queries to verify that designated time servers peered with one another to keep consistent and accurate time. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
	● Systems receive time only from designated central time server(s).	360 Advanced inspected time configuration settings and time queries to verify that systems received time information only from designated central time servers. NTP settings are configured to use Amazon Web Services with time.windows.com as a secondary source. Documentation Reviewed: SRV-01.7 Server NTP Settings SRV-02 Server Hardening Scripts & Security Enforcement http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html					
10.4.2 Time data is protected.			☒	☐	☐	☐	☐
10.4.2.a Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.	*For all items in the sample from 10.4.1,* **describe how** configuration settings verified that access to time data is restricted to only personnel with a business need to access time data.	360 Advanced inspected user access configurations to verify that time data was restricted to personnel who have business need to access time data. User listings and permissions indicated that only designated systems administrators were permitted access to time data settings. Documentation Reviewed: SRV-01.1 Server User Listing & Access Permissions					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.4.2.b Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	*For all items in the sample from 10.4.1,* **describe how** configuration settings and time synchronization settings verified that any changes to time settings on critical systems are logged.	360 Advanced inspected system audit policies and log samples to verify that any changes to time settings on critical systems were logged. Audit policies included logging of security state changes which comprised of changes made to time settings. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
	For all items in the sample from 10.4.1, **describe how** the examined logs verified that any changes to time settings on critical systems are logged.	360 Advanced inspected system audit policies and log samples to verify that any changes to time settings on critical systems were logged. Audit policies were configured to log security state changes which included changes made to time settings. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
	Describe how time synchronization processes were examined to verify changes to time settings on critical systems are:						
	• Logged	360 Advanced inspected system audit policies and log samples to verify that any changes to time settings on critical systems were logged. Audit policies were configured to log security state changes which included changes made to time settings. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor to log and correlate system activity. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Monitored	360 Advanced inspected system audit policies and log samples to verify that any changes to time settings on critical systems were monitored. Audit policies included logging of security state changes which comprised of changes made to time settings. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor which was monitored and reviewed by systems administrators and security personnel through the AlienVault console. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
	• Reviewed	360 Advanced inspected system audit policies and log samples to verify that any changes to time settings on critical systems were reviewed. Audit policies included logging of security state changes which comprised of changes made to time settings. Either syslog services or AlienVault agents were configured locally on system components to forward these event types to the AlienVault USM Anywhere Sensor which was monitored and reviewed by systems administrators and security personnel through the AlienVault console. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
10.4.3 Time settings are received from industry-accepted time sources.			☒	☐	☐	☐	☐
10.4.3 Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted	**Identify the sample** of time servers selected for this testing procedure.	Sample Set-1: Servers					
	For all items in the sample, **describe how** configuration settings verified either of the following:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	• That the time servers receive time updates from specific, industry-accepted external sources. OR	360 Advanced inspected time configuration settings and time queries to verify that the designated centralized time servers located and operated by Amazon were configured to sync time from the following industry-accepted external sources: - server 0.amazon.pool.ntp.org iburst - server 1.amazon.pool.ntp.org iburst - server 2.amazon.pool.ntp.org iburst - server 3.amazon.pool.ntp.org iburst					
	• That time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines.	Not Applicable. Fairfax did not encrypt time updates but instead synchronized system time with specific, industry-accepted external time sources.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.5 Secure audit trails so they cannot be altered.			☒	☐	☐	☐	☐
10.5 Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:	**Identify the system administrators** interviewed who confirm that audit trails are secured so that they cannot be altered as follows (from 10.5.1-10.5.5): ● Only individuals who have a job-related need can view audit trail files. ● Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. ● Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, including: - That current audit trail files are promptly backed up to the centralized log server or media - The frequency that audit trail files are backed up - That the centralized log server or media is difficult to alter ● Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. ● Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.	Alex Umansky - Senior Software Engineer				
	Identify the sample of system components selected for 10.5.1-10.5.5.	Sample Set-1: Servers					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.5.1 Limit viewing of audit trails to those with a job-related need.			☒	☐	☐	☐	☐
10.5.1 Only individuals who have a job-related need can view audit trail files.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that only individuals who have a job-related need can view audit trail files.	360 Advanced inspected configuration settings for the sample of system components to verify that user rights and permissions restricted viewing of audit files to only individuals who have a documented job-related need. Viewing of raw audit logs on servers were restricted only to systems administrators and security personnel while access to the AlienVault and AWS management console was provisioned using individual user accounts based on job-related needs. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA LOG-01 Central Log System - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions					
10.5.2 Protect audit trail files from unauthorized modifications.			☒	☐	☐	☐	☐
10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	360 Advanced inspected configuration settings for the sample of system components to verify that current audit trail files were protected from unauthorized modifications. Viewing of raw audit logs on servers were restricted only to systems administrators and security personnel while access to the AlienVault and AWS management console was provisioned using individual user accounts based on job-related needs. Log events from servers and network devices were forwarded to the AlienVault USM Anywhere Sensor for storage and optimized log searching. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment. Logs are only displayed in read-only mode and cannot be modified by end users. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA LOG-01 Central Log System - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions SRV-02 Server Hardening Scripts & Security Enforcement					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.			☒	☐	☐	☐	☐
10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	360 Advanced inspected configuration settings and log entries for the sample of system components to verify that real-time audit logs were forwarded and written onto a secure, centralized, internal log server. Log events from servers and network devices were forwarded to the AlienVault USM Anywhere Sensor for storage and optimized log searching. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment. Logs are only displayed in read-only mode and cannot be modified by end users. Documentation Reviewed: AWS-01 AWS IAM - User Listing & Access Permissions & MFA LOG-01 Central Log System - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions SRV-02 Server Hardening Scripts & Security Enforcement					
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.			☒	☐	☐	☐	☐
10.5.4 Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that logs for external-facing technologies are written onto a secure, centralized, internal log server or media.	360 Advanced inspected configuration settings and log entries for the sample of system components to verify that real-time audit logs were forwarded and written onto a secure, centralized, internal log server. Log events from servers and network devices were forwarded to the AlienVault USM Anywhere Sensor for storage and optimized log searching. In addition, AWS CloudTrail and CloudWatch services were enabled to log user and resource activity and to gain system-wide visibility into resource utilization, application performance, and operational health within the AWS environment. Logs are only displayed in read-only mode and cannot be modified by end users. Documentation Reviewed: LOG-01 Central Log System - User Listing & Permissions SRV-01.1 Server User Listing & Access Permissions AWS-01 AWS IAM - User Listing & Access Permissions & MFA SRV-02 Server Hardening Scripts & Security Enforcement					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).			☒	☐	☐	☐	☐
10.5.5 Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.	*For each item in the sample at 10.5,* **describe how** the following verified the use of file-integrity monitoring or change-detection software on logs:						
	• System settings	360 Advanced inspected system settings to verify that audit policies and file-integrity software were configured to monitor log files. Trend Micro Deep Security agents were used to monitor system and log file changes and configured to forward events to the centralized Deep Security Manager server which was monitored and reviewed by systems administrators and security personnel through the Deep Security Management console. Documentation Reviewed: FIM-01 FIM - Monitored Files & Comparison Schedule					
	• Monitored files	360 Advanced inspected system settings to verify that audit policies and file-integrity software were configured to monitor log files. Trend Micro Deep Security agents were used to monitor system and log file changes and configured to forward events to the centralized Deep Security Manager server which was monitored and reviewed by systems administrators and security personnel through the Deep Security Management console. Documentation Reviewed: FIM-01 FIM - Monitored Files & Comparison Schedule					
	• Results from monitoring activities	360 Advanced inspected example FIM logs to verify that audit policies and file-integrity software were configured to monitor log files. Trend Micro Deep Security agents were used to monitor system and log file changes and configured to forward events to the centralized Deep Security Manager server which was monitored and reviewed by systems administrators and security personnel through the Deep Security Management console. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples					
	Identify the file-integrity monitoring (FIM) or change-detection software verified to be in use.	Trend Micro Deep Security 12					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*							
10.6 Perform the following:							
10.6.1 Review the following at least daily: ● All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).			☒	☐	☐	☐	☐
10.6.1.a Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools: ● All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools: ● All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions.	POL-01 Data Security Policies and Procedures					
	Describe the manual or log tools used for daily review of logs.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that log tools were utilized to correlate and alert personnel on security events for all systems within the environment. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: ● All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	**Identify the responsible personnel** interviewed who confirm that the following are reviewed at least daily: ● All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions.	Alex Umansky - Senior Software Engineer					
	Describe how processes were observed to verify that the following are reviewed at least daily:						
	● All security events.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that all security events were reviewed at least daily. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server. These management servers automatically correlate events and alert responsible personnel for any action to be taken including the creation of issue-tracking tickets or the initiation of the incident response process in the event that a security incident is detected. The management consoles also provide dashboards of metrics and notification logs that are monitored and reviewed by system administrators and security personnel. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Logs of all system components that store, process, or transmit CHD and/or SAD.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that logs from all systems that store, process, or transmit CHD were reviewed at least daily. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server. These management servers automatically correlate events and alert responsible personnel for any action to be taken including the creation of issue-tracking tickets or the initiation of the incident response process in the event that a security incident is detected. The management consoles also provide dashboards of metrics and notification logs that are monitored and reviewed by system administrators and security personnel. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
	• Logs of all critical system components.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that logs from all critical system components were reviewed at least daily. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server. These management servers automatically correlate events and alert responsible personnel for any action to be taken including the creation of issue-tracking tickets or the initiation of the incident response process in the event that a security incident is detected. The management consoles also provide dashboards of metrics and notification logs that are monitored and reviewed by system administrators and security personnel. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Logs of all servers and system components that perform security functions.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that logs from all system components that perform security functions such as anti-virus, IDS, and FIM were reviewed at least daily. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server. These management servers automatically correlate events and alert responsible personnel for any action to be taken including the creation of issue-tracking tickets or the initiation of the incident response process in the event that a security incident is detected. The management consoles also provide dashboards of metrics and notification logs that are monitored and reviewed by system administrators and security personnel. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.			☒	☐	☐	☐	☐
10.6.2.a Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the	**Identify the documented security policies and procedures** examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
organization's policies and risk management strategy.	**Describe the manual or log tools** defined for periodic review of logs of all other system components.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that logs from all other system components were reviewed periodically. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server. These management servers automatically correlate events and alert responsible personnel for any action to be taken including the creation of issue-tracking tickets or the initiation of the incident response process in the event that a security incident is detected. The management consoles also provide dashboards of metrics and notification logs that are monitored and reviewed by system administrators and security personnel. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
10.6.2.b Examine the organization's risk assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.	**Identify the organization's risk assessment documentation** examined to verify that reviews are performed in accordance with the organization's policies and risk management strategy.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that reviews are performed in accordance with organization's policies and risk management strategy.	Nadine Chahal - General Counsel					
10.6.3 Follow up exceptions and anomalies identified during the review process.			☒	☐	☐	☐	☐
10.6.3.a Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.	**Identify the documented security policies and procedures** examined to verify that procedures define following up on exceptions and anomalies identified during the review process.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.	**Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that all security events were reviewed at least daily. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server. These management servers automatically correlate events and alert responsible personnel for any action to be taken including the creation of issue-tracking tickets or the initiation of the incident response process in the event that a security incident is detected. The management consoles also provide dashboards of metrics and notification logs that are monitored and reviewed by system administrators and security personnel.					
	Identify the responsible personnel interviewed who confirm that follow-up to exceptions and anomalies is performed.	Alex Umansky - Senior Software Engineer					
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).			☒	☐	☐	☐	☐
10.7.a Examine security policies and procedures to verify that they define the following: ● Audit log retention policies. ● Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.	**Identify the documented security policies and procedures** examined to verify that procedures define the following: ● Audit log retention policies. ● Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.	POL-01 Data Security Policies and Procedures					
10.7.b Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.	**Identify the responsible personnel** interviewed who confirm that audit logs are retained for at least one year.	Alex Umansky - Senior Software Engineer					
	Describe how the audit logs verified that audit logs are retained for at least one year.	360 Advanced inspected a sample of filtered events to verify that audit logs were available for at least one year. Documentation Reviewed: LOG-02 Central Log System - Log Retention					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.7.c Interview personnel and observe processes to verify that at least the last three months' logs are immediately available for analysis.	**Identify the responsible personnel** interviewed who confirm that at least the last three months' logs are immediately available for analysis.	Alex Umansky - Senior Software Engineer					
	Describe how processes were observed to verify that at least the last three months' logs are immediately available for analysis.	360 Advanced observed the AlienVault and Deep Security Manager dashboards to verify that audit logs of at least the last three months were immediately available for analysis. Logs were observed to be immediately available for at least a year using the date filtering function within the log view dashboards.					
10.8 ***Additional requirement for service providers only:*** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)			☒	☐	☐	☐	☐
10.8.a Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:. • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	**Identify the documented policies and procedures** examined to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:. • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	POL-01 Data Security Policies and Procedures LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.8.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	**Identify the responsible personnel** interviewed who confirm that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	Nadine Chahal - General Counsel					
	Describe how the detection and alerting processes verified that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	360 Advanced inspected audit log settings and observed log monitoring dashboards to verify that all security events were reviewed at least daily. Syslog services or AlienVault agent software were installed and configured to forward security-related events to the AlienVault USM Anywhere Sensor to log and correlate system activity. Trend Micro Deep Security agent software were installed and configured to forward anti-virus, intrusion detection, and file-integrity monitoring logs to the Deep Security Manager server. These management servers automatically correlate events and alert responsible personnel for any action to be taken including the creation of issue-tracking tickets or the initiation of the incident response process in the event that a security incident is detected. The management consoles also provide dashboards of metrics and notification logs that are monitored and reviewed by system administrators and security personnel. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.8.1 ***Additional requirement for service providers only:*** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: ● Restoring security functions ● Identifying and documenting the duration (date and time start to end) of the security failure ● Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause ● Identifying and addressing any security issues that arose during the failure ● Performing a risk assessment to determine whether further actions are required as a result of the security failure ● Implementing controls to prevent cause of failure from reoccurring ● Resuming monitoring of security controls			☒	☐	☐	☐	☐
10.8.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: ● Restoring security functions ● Identifying and documenting the duration (date and time start to end) of the security failure ● Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause ● Identifying and addressing any security issues that arose during the failure	**Identify the documented policies and procedures** examined to verify that processes are defined and implemented to respond to a security control failure, and include: ● Restoring security functions ● Identifying and documenting the duration (date and time start to end) of the security failure ● Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause ● Identifying and addressing any security issues that arose during the failure ● Performing a risk assessment to determine whether further actions are required as a result of the security failure ● Implementing controls to prevent cause of failure from reoccurring ● Resuming monitoring of security controls	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	**Identify the responsible personnel** interviewed who confirm that processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
10.8.1.b Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	**Identify the sample of records** examined to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	No security incidents or security control failures occurred within the audit period assessed. However, 360 Advanced inspected policies and test plans which indicated that documentation of the duration, identification, and remediation of the security incident or control failure were to be included with the root cause of the issue. Documentation Reviewed: AS-04.2 Incident Response Testing & Training POL-01 Data Security Policies and Procedures					
	For each sampled record, **describe how** the documented security control failures include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	No security incidents or security control failures occurred within the audit period assessed. However, 360 Advanced inspected policies and test plans which indicated that documentation of the duration, identification, and remediation of the security incident or control failure were to be included with the root cause of the issue. Documentation Reviewed: AS-04.2 Incident Response Testing & Training POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
10.9 Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are: ● Documented, ● In use, and ● Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented.	POL-01 Data Security Policies and Procedures RVW-05 Review of Operational Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for monitoring all access to network resources and cardholder data are: ● In use ● Known to all affected parties	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					

Requirement 11: Regularly test security systems and processes

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.			☒	☐	☐	☐	☐
11.1.a Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis.	**Identify the documented policies and procedures** examined to verify processes are defined for detection and identification of authorized and unauthorized wireless access points on a quarterly basis.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: ● WLAN cards inserted into system components. ● Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). ● Wireless devices attached to a network port or network device.	**Provide the name of the assessor** who attests that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: ● WLAN cards inserted into system components. ● Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). ● Wireless devices attached to a network port or network device.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
11.1.c If wireless scanning is utilized, examine output from recent wireless scans to verify that: ● Authorized and unauthorized wireless access points are identified, and ● The scan is performed at least quarterly for all system components and facilities.	**Indicate whether** wireless scanning is utilized. **(yes/no)** *If 'no,' mark the remainder of 11.1.c as 'not applicable.'*	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	If 'yes,' **Identify/describe** the output from recent wireless scans examined to verify that: ● Authorized wireless access points are identified. ● Unauthorized wireless access points are identified. ● The scan is performed at least quarterly. ● The scan covers all system components. ● The scan covers all facilities.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel.	**Indicate whether** automated monitoring is utilized. **(yes/no)**	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	If "no," mark the remainder of 11.1.d as "Not Applicable." *If "yes," complete the following:*						
	Identify and describe any automated monitoring technologies in use.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	For each monitoring technology in use, **describe how** the technology generates alerts to personnel.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.			☒	☐	☐	☐	☐
11.1.1 Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.	**Identify the documented inventory records** of authorized wireless access points examined to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.			☒	☐	☐	☐	☐
11.1.2.a Examine the organization's incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected.	**Identify the Incident Response Plan document** examined that defines and requires response in the event that an unauthorized wireless access point is detected.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.1.2.b Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found.	**Identify the responsible personnel** interviewed for this testing procedure.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	For the interview, **summarize the relevant details** discussed that verify that action is taken when unauthorized wireless access points are found.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	And/or:						
	Identify the recent wireless scans inspected for this testing procedure.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					
	Describe how the recent wireless scans and related responses verified that action is taken when unauthorized wireless access points are found.	Fairfax's cardholder data environment resided solely within their hosted infrastructure provided by Amazon Web Services, a PCI-compliant Level-1 service provider, who included these testing procedures in their own PCI assessment. Fairfax reviews the Attestation of Compliance for AWS (currently dated June 10, 2021, against PCI DSS v3.2.1) on an annual basis to ensure that compliance is maintained for this requirement. Documentation Reviewed: SP-02 Service Provider Third-Party Auditor Reports					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*			☒	☐	☐	☐	☐
11.2 Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as follows:							
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high-risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.			☒	☐	☐	☐	☐
11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.	**Identify the internal vulnerability scan reports and supporting documentation** reviewed.	SCN-01 Internal Vulnerability Scans					
	Provide the name of the assessor who attests that four quarterly internal scans were verified to have occurred in the most recent 12-month period.	Phillip Hagan, QSA# 204-876					
11.2.1.b Review the scan reports and verify that all "high-risk" vulnerabilities are addressed and the scan process includes rescans to verify that the "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	**Identify the documented process for quarterly internal scanning** to verify the process defines performing rescans as part of the quarterly internal scan process.	POL-01 Data Security Policies and Procedures					
	For each of the four internal quarterly scans indicated at 11.2.1.a, **indicate whether** a rescan was required. **(yes/no)**	Yes.					
	If "yes," **describe how** rescans were verified to be performed until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	Internal vulnerability scans are currently conducted monthly. SCN-01 Internal Vulnerability Scan Results indicate "high-risk" vulnerabilities were detected during the internal vulnerability scans performed against the deepwatch networks. Subsequent internal vulnerability scans show the number of vulnerabilities changing monthly showing that remediation efforts seemed to be in place.					
11.2.1.c Interview personnel to verify that the scan was performed by a qualified	**Identify the responsible personnel** interviewed for this testing procedure.	Alex Umansky - Senior Software Engineer					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Indicate whether** a qualified internal resource performs the scan. **(yes/no)** *If "no," mark the remainder of 11.2.1.c as "Not Applicable."* *If "yes," complete the following:*	No.					
	For the interview, **summarize the relevant details** discussed that verify:						
	● The scan was performed by a qualified internal resource	Not Applicable. Internal scans were performed through AlienVault, a qualified external third-party vendor.					
	● Organizational independence of the tester exists.	Not Applicable. Internal vulnerability scans were performed by AlienVault, an independent organization who was not involved in the design, development, and implementation of the system components scanned.					
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*			☒	☐	☐	☐	☐
11.2.2.a Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period.	**Identify the external network vulnerability scan reports and supporting documentation** reviewed.	SCN-02 External Vulnerability Scans					
	Provide the name of the assessor who attests that four quarterly external vulnerability scans were verified to have occurred in the most recent 12-month period.	Phillip Hagan, QSA# 204-876					
11.2.2.b Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures).	**Provide the name of the assessor** who attests that the results of each quarterly scan were reviewed and verified that the ASV Program Guide requirements for a passing scan have been met.	Phillip Hagan, QSA# 204-876					
	For each of the four external quarterly scans indicated at 11.2.2.a, **indicate whether** a rescan was necessary. **(yes/no)**	Yes.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	If "yes," **describe how** the results of the rescan verified that the ASV Program Guide requirements for a passing scan have been met.	Failed scan was a result of false positive findings of the lisadmin Directory Present Vulnerability and Reference to Windows file path is present in HTML (December 2, 2020). All issues have been resolved and achievement of passing scores were indicated in the remediation scans performed on March 3, 2021.					
11.2.2.c Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	**Provide the name of the assessor** who attests that the external scan reports were reviewed and verified to have been completed by a PCI SSC-Approved Scanning Vendor (ASV).	Phillip Hagan, QSA# 204-878					
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.			☒	☐	☐	☐	☐
11.2.3.a Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned.	**Identify the change control documentation and scan reports** reviewed for this testing procedure.	CHG-05 Change Records - Significant Changes to Environment SCN-03 Significant Changes - Internal Vulnerability Scans SCN-04 Significant Changes - External Vulnerability Scans					
	Describe how the change control documentation and scan reports verified that all system components subject to significant change were scanned after the change.	360 inspected change request tickets and internal and external vulnerability scans completed after the significant changes occurred. A new client environment was implemented requiring new servers installed and ports opened for the client's web application. Work was completed on December 20, 2020. Documentation Reviewed: CHG-05 Change Records - Significant Changes to Environment SCN-03 Significant Changes - Internal Vulnerability Scans SCN-04 Significant Changes - External Vulnerability Scans					
11.2.3.b Review scan reports and verify that the scan process includes rescans until: ● For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. ● For internal scans, all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	For all scans reviewed in 11.2.3.a, **indicate whether** a rescan was required. **(yes/no)**	Yes.					
	If "yes" – for external scans, **describe how** rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist.	High vulnerabilities were addressed and an external scan was performed by Qualys three days after the failed scan. The rescan indicated a passing compliance status with no high vulnerabilities noted.					
	If "yes" – for internal scans, **describe how** rescans were performed until either passing results were obtained or all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved.	Rescans indicated a reduced number of high vulnerabilities as remediation efforts were implemented. The most recent quarterly internal scan performed by AlienVault indicated thee no high vulnerabilities.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Indicate whether** an internal resource performed the scans. **(yes/no)** *If "no," mark the remainder of 11.2.3.c as "Not Applicable."* *If "yes," complete the following:*	No.					
	Describe how the personnel who perform the scans demonstrated they are qualified to perform the scans.	Not Applicable. Internal vulnerability scans were performed by AlienVault and external vulnerability scans were performed by Qualys. Both AlienVault and Qualys are qualified external third-party vendors.					
	Describe how organizational independence of the tester was observed to exist.	Not Applicable. Internal vulnerability scans were performed by AlienVault and external vulnerability scans were performed by Qualys. Both AlienVault and Qualys are an independent organizations who were not involved in the design, development, and implementation of the system components scanned.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.3 Implement a methodology for penetration testing that includes at least the following: ● Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). ● Includes coverage for the entire CDE perimeter and critical systems. ● Includes testing from both inside and outside of the network. ● Includes testing to validate any segmentation and scope reduction controls. ● Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. ● Defines network-layer penetration tests to include components that support network functions as well as operating systems. ● Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. ● Specifies retention of penetration testing results and remediation activities results.			☒	☐	☐	☐	☐
11.3 Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented and includes at least the following: ● Is based on industry-accepted penetration testing approaches. ● Includes coverage for the entire CDE perimeter and critical systems. ● Includes testing from both inside and outside the network. ● Includes testing to validate any segmentation and scope reduction controls. ● Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. ● Defines network-layer penetration tests to include components that support	**Identify the documented penetration-testing methodology** examined to verify a methodology is implemented that includes at least the following: ● Based on industry-accepted penetration testing approaches. ● Coverage for the entire CDE perimeter and critical systems. ● Testing from both inside and outside the network. ● Testing to validate any segmentation and scope reduction controls. ● Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. ● Defines network-layer penetration tests to include components that support network functions as well as operating systems. ● Review and consideration of threats and vulnerabilities experienced in the last 12 months. ● Retention of penetration testing results and remediation activities results.	AS-02.1 External & Internal Pen Test & Remediation				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
network functions as well as operating systems. ● Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. ● Specifies retention of penetration testing results and remediation activities results.	**Identify the responsible personnel** interviewed who confirm the penetration–testing methodology implemented includes at least the following: ● Based on industry-accepted penetration testing approaches. ● Coverage for the entire CDE perimeter and critical systems. ● Testing from both inside and outside the network. ● Testing to validate any segmentation and scope reduction controls. ● Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. ● Defines network-layer penetration tests to include components that support network functions as well as operating systems. ● Review and consideration of threats and vulnerabilities experienced in the last 12 months. ● Retention of penetration testing results and remediation activities results.	Alex Umansky - Senior Software Engineer					
11.3.1 Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).			☒	☐	☐	☐	☐
11.3.1.a Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: ● Per the defined methodology ● At least annually ● After any significant changes to the environment	**Identify the documented external penetration test results** reviewed to verify that external penetration testing is performed: ● Per the defined methodology ● At least annually	AS-02.1 External & Internal Pen Test & Remediation					
	Describe how the scope of work verified that external penetration testing is performed: ● Per the defined methodology ● At least annually	360 Advanced inspected the penetration test report to verify that testing was performed per the defined methodology and at least annually. Content within the report included information as defined in Requirement 11.3. In addition, the previous and current penetration tests were provided to indicate that tests are performed on an annual basis.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify whether any significant external infrastructure or application upgrade or modification occurred during the past 12 months. **(yes/no)**	Not Applicable. While the significant change did not warrant an external penetration test, Fairfax completes monthly external vulnerability scans and quarterly ASV external vulnerability scans. Since the significant change occurred on October 2020, there have been quarterly ASV scans, quarterly firewall/security group reviews, and external and internal penetration tests that occurred July 2021.					
	Identify the documented penetration test results reviewed to verify that external penetration tests are performed after significant external infrastructure or application upgrade.	AS-02.1 External & Internal Pen Test & Remediation					
11.3.1.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Indicate whether** an internal resource performed the test. **(yes/no)** *If "no," mark the remainder of 11.3.1.b as "Not Applicable."* *If "yes," complete the following:*	No.					
	Describe how the personnel who perform the penetration tests demonstrated they are qualified to perform the tests.	Not Applicable. The external penetration test was performed by 360 Advanced, an independent organization that specializes in information security and penetration testing.					
	Describe how organizational independence of the tester was observed to exist.	Not Applicable. The external penetration test was performed by 360 Advanced, an independent organization that specializes in information security and penetration testing.					
11.3.2 Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).			☒	☐	☐	☐	☐
11.3.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows: ● Per the defined methodology	**Identify the documented internal penetration test results** reviewed to verify that internal penetration testing is performed: ● Per the defined methodology ● At least annually	AS-02.1 External & Internal Pen Test & Remediation					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● At least annually ● After any significant changes to the environment	**Describe how** the scope of work verified that internal penetration testing is performed: ● Per the defined methodology ● At least annually	360 Advanced inspected the penetration test report to verify that testing was performed per the defined methodology and at least annually. Content within the report included information as defined in Requirement 11.3. In addition, the previous and current penetration tests were provided to indicate that tests are performed on an annual basis.					
	Indicate whether any significant internal infrastructure or application upgrade or modification occurred during the past 12 months. **(yes/no)**	Not Applicable. While the significant change did not warrant an external penetration test, Fairfax completes monthly external vulnerability scans and quarterly ASV external vulnerability scans. Since the significant change occurred on October 2020, there have been quarterly ASV scans, quarterly firewall/security group reviews, and external and internal penetration tests that occurred July 2021.					
	Identify the documented internal penetration test results reviewed to verify that internal penetration tests are performed after significant internal infrastructure or application upgrade.	AS-02.1 External & Internal Pen Test & Remediation					
11.3.2.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Indicate whether** an internal resource performed the test. **(yes/no)** *If "no," mark the remainder of 11.3.2.b as "Not Applicable."* *If "yes," complete the following:*	No.					
	Describe how the personnel who perform the penetration tests demonstrated they are qualified to perform the tests	Not Applicable. The internal penetration test was performed by 360 Advanced, an independent organization that specializes in information security and penetration testing.					
	Describe how organizational independence of the tester was observed to exist.	Not Applicable. The internal penetration test was performed by 360 Advanced, an independent organization that specializes in information security and penetration testing.					
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.			☒	☐	☐	☐	☐
11.3.3 Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	**Identify the documented penetration testing results** examined to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	AS-02.1 External & Internal Pen Test & Remediation					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.			☐	☐	☒	☐	☐
11.3.4.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**Indicate whether** segmentation is used to isolate the CDE from other networks. **(yes/no)** *If "no," mark the remainder of 11.3.4.a and 11.3.4.b as "Not Applicable."*	No.					
	If "yes," **identify the defined penetration-testing methodology** examined to verify procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					
	Describe how the segmentation controls verified that segmentation methods:						
	• Are operational and effective.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					
	• Isolate all out-of-scope systems from systems in the CDE.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					
11.3.4.b Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**Identify the documented results from the most recent penetration test** examined to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.3.4.c Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					
	Describe how organizational independence of the tester was observed to exist.	Organizational independence of the testers was observed to exist since they were not involved in the design, development, and implementation of the system components scanned.					
11.3.4.1 ***Additional requirement for service providers only:*** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.			☐	☐	☒	☐	☐
11.3.4.1.a Examine the results from the most recent penetration test to verify that: ● Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. ● The penetration testing covers all segmentation controls/methods in use. ● The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**Identify the documented results from the most recent penetration test** examined to verify that: ● Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. ● The penetration testing covers all segmentation controls/methods in use. ● The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					
11.3.4.1.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					
	Describe how organizational independence of the tester was observed to exist.	Not Applicable. Segmentation was not used to isolate the CDE from other networks. The CDE was solely hosted within the AWS cloud environment in which all system components were considered to be in scope and included for this assessment.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.4 Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.			☒	☐	☐	☐	☐
11.4.a Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: ● At the perimeter of the cardholder data environment. ● At critical points in the cardholder data environment.	**Identify the network diagrams** examined to verify that techniques are in place to monitor all traffic: ● At the perimeter of the cardholder data environment. ● At critical points in the cardholder data environment.	DGM-01 Network Diagrams DGM-02 Data Flow Diagrams					
	Describe how system configurations verified that techniques are in place to monitor all traffic:						
	● At the perimeter of the cardholder data environment.	360 Advanced inspected the Trend Micro Deep Security Manager configurations to verify that techniques were in place to monitor all traffic at the perimeter of the CDE. The Trend Micro Deep Security agent was installed on each individual system component and configured to monitor all inbound and outbound host traffic. Monitoring of all systems provided a full view on data flows and access attempts throughout the entire CDE. Documentation Reviewed: IDS-01 IDS - Rule Sets & Signature Updates					
	● At critical points in the cardholder data environment.	360 Advanced inspected the Trend Micro Deep Security Manager configurations to verify that techniques were in place to monitor all traffic at critical points in the CDE. The Trend Micro Deep Security agent was installed on each individual system component and configured to monitor all inbound and outbound host traffic. Monitoring of all systems provided a full view on data flows and access attempts throughout the entire CDE. Documentation Reviewed: IDS-01 IDS - Rule Sets & Signature Updates					
11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	**Describe how** system configurations for intrusion-detection and/or intrusion-prevention techniques verified that they are configured to alert personnel of suspected compromises.	360 Advanced inspected the Trend Micro Deep Security Manager and AlienVault USM platform configurations to verify that settings were configured to alert personnel of suspected compromises. Documentation Reviewed: IDS-01 IDS - Rule Sets & Signature Updates LOG-04 Central Log System - Alert Settings & Examples					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed who confirm that the generated alerts are received as intended.	Alex Umansky - Senior Software Engineer					
11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	**Identify the vendor document(s)** examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques.	Trend Micro Business Support - Deep Security 10.0: https://success.trendmicro.com/product-support/deep-security-12-0					
	Describe how IDS/IPS configurations and vendor documentation verified that intrusion-detection, and/or intrusion-prevention techniques are:						
	● Configured per vendor instructions to ensure optimal protection.	360 Advanced inspected the Trend Micro Deep Security Manager and compared them to vendor documentation to verify that intrusion-prevention techniques were configured per vendor instructions to ensure optimal protection against intrusion and malicious attempts. Documentation Reviewed: IDS-01 IDS - Rule Sets & Signature Updates					
	● Maintained per vendor instructions to ensure optimal protection.	360 Advanced inspected the Trend Micro Deep Security Manager configurations and compared them to vendor documentation to verify that intrusion-prevention techniques were maintained per vendor instructions to ensure optimal protection against intrusion and malicious attempts. Documentation Reviewed: IDS-01 IDS - Rule Sets & Signature Updates					
	● Updated per vendor instructions to ensure optimal protection.	360 Advanced inspected the Trend Micro Deep Security Manager configurations and compared them to vendor documentation to verify that intrusion-prevention techniques were updated per vendor instructions to ensure optimal protection against intrusion and malicious attempts. Documentation Reviewed: IDS-01 IDS - Rule Sets & Signature Updates					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*			☒	☐	☐	☐	☐
11.5.a Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. ● Examples of files that should be monitored: ● System executables ● Application executables ● Configuration and parameter files ● Centrally stored, historical or archived, log and audit files ● Additional critical files determined by entity (i.e., through risk assessment or other means)	**Describe** the change-detection mechanism deployed.	Trend Micro Deep Security					
	Identify the results from monitored files reviewed to verify the use of a change-detection mechanism.	LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples FIM-01 FIM - Monitored Files & Comparison Schedule					
	Describe how the following verified the use of a change-detection mechanism:						
	● System settings	360 Advanced inspected the Trend Micro Deep Security Manager and its host-based agent services to verify that settings were configured to monitor unauthorized modification of critical system files. Documentation Reviewed: FIM-01 FIM - Monitored Files & Comparison Schedule SRV-01.3 Server Running Services & Listening Ports SRV-01.4 Server Installed Applications & Versions					
	● Monitored files	360 Advanced inspected the Trend Micro Deep Security Manager and its host-based agent services to verify that settings were configured to monitor unauthorized modification of files configured to be monitored. Documentation Reviewed: FIM-01 FIM - Monitored Files & Comparison Schedule SRV-01.3 Server Running Services & Listening Ports SRV-01.4 Server Installed Applications & Versions					
	Describe how system settings verified that the change-detection mechanism is configured to:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.5.b Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly.	• Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files.	360 Advanced inspected the Trend Micro Deep Security Manager and its host-based agent services to verify that any file integrity discrepancies discovered during the monitoring of critical directories and files were logged and an alert generated via email to security personnel. Documentation Reviewed: FIM-01 FIM - Monitored Files & Comparison Schedule SRV-01.3 Server Running Services & Listening Ports SRV-01.4 Server Installed Applications & Versions					
	• Perform critical file comparisons at least weekly.	360 Advanced inspected the Trend Micro Deep Security Manager and its host-based agent services to verify that settings were configured to perform file comparisons in real-time and alert personnel to unauthorized modification of critical files. Documentation Reviewed: FIM-01 FIM - Monitored Files & Comparison Schedule					
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.			☒	☐	☐	☐	☐
11.5.1 Interview personnel to verify that all alerts are investigated and resolved.	**Identify the responsible personnel** interviewed who confirm that all alerts are investigated and resolved,	Alex Umansky - Senior Software Engineer					
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
11.6 Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for security monitoring and testing are documented.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for security monitoring and testing are: • In use • Known to all affected parties	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.1 Establish, publish, maintain, and disseminate a security policy.			☒	☐	☐	☐	☐
12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	**Identify the documented information security policy** examined.	POL-01 Data Security Policies and Procedures					
	Describe how the information security policy was verified to be published and disseminated to:						
	• All relevant personnel.	360 Advanced inspected policies and a sample of signed annual training acknowledgements performed during security awareness training to verify that the security policy was provided to all relevant personnel with access to cardholder data upon hire and annually thereafter. Documentation Reviewed: SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing) EMP-02.1 Employee Annual Security Awareness Refresher POL-00 Dissemination of Policies & Procedures					
	• All relevant vendors and business partners.	Not Applicable. Fairfax did not have vendors or business partners with access to the cardholder data environment.					
12.1.1 Review the security policy at least annually and update the policy when business objectives or the risk environment change.			☒	☐	☐	☐	☐
12.1.1 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.	**Describe how** the information security policy was verified to be:						
	• Reviewed at least annually.	360 Advanced inspected the revision history table within the information security policy to verify that the document was reviewed at least annually. The revision history indicated incremental modifications over the life of the document including the latest review and update occurring within the last year. Documentation Reviewed: POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Updated as needed to reflect changes to business objectives or the risk environment.	360 Advanced inspected the revision history table within the information security policy to verify that the document was updated as needed to reflect changes to business objectives or the risk environment. The revision history indicated incremental modifications over the life of the document including significant updates to reflect new changes and risks to the organization's environment. Documentation Reviewed: POL-01 Data Security Policies and Procedures					
12.2 Implement a risk assessment process, that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*			☒	☐	☐	☐	☐
12.2.a Verify that an annual risk-assessment process is documented that: • Identifies critical assets, threats, and vulnerabilities • Results in a formal, documented analysis of risk.	**Provide the name of the assessor** who attests that the documented annual risk-assessment process: • Identifies critical assets, threats, and vulnerabilities • Results in a formal, documented analysis of risk.	Phillip Hagan, QSA# 204-876					
12.2.b Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	**Identify the risk assessment result documentation** reviewed to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	AS-01 Risk Assessment Result Documentation POL-01 Data Security Policies and Procedures					
12.3 Develop usage policies for critical technologies and define proper use of these technologies. ***Note:*** *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following:			☒	☐	☐	☐	☐
12.3 Examine the usage policies for critical technologies and interview responsible personnel to verify the	**Identify critical technologies in use.**	Critical technologies in use include servers, workstations, laptops, software, and all internal and external communications including e-mail, remote access, and Internet access.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
following policies are implemented and followed:	**Identify the usage policies for all identified critical technologies** reviewed to verify the following policies (12.3.1-12.3.10) are defined: ● Explicit approval from authorized parties to use the technologies. ● All technology use to be authenticated with user ID and password or other authentication item. ● A list of all devices and personnel authorized to use the devices. ● A method to accurately and readily determine owner, contact information, and purpose. ● Acceptable uses for the technology. ● Acceptable network locations for the technology. ● A list of company-approved products. ● Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. ● Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. ● Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed who confirm usage policies for all identified critical technologies are implemented and followed (for 12.3.1–12.3.10): ● Explicit approval from authorized parties to use the technologies. ● All technology use to be authenticated with user ID and password or other authentication item. ● A list of all devices and personnel authorized to use the devices. ● A method to accurately and readily determine owner, contact information, and purpose. ● Acceptable uses for the technology. ● Acceptable network locations for the technology. ● A list of company-approved products. ● Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. ● Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. ● Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
12.3.1 Explicit approval by authorized parties.			☒	☐	☐	☐	☐
12.3.1 Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies.	**Provide the name of the assessor** who attests that the usage policies were verified to include processes for explicit approval from authorized parties to use the technologies.	Phillip Hagan, QSA# 204-876					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.3.2 Authentication for use of the technology.			☒	☐	☐	☐	☐
12.3.2 Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token).	**Provide the name of the assessor** who attests that the usage policies were verified to include processes for all technology use to be authenticated with user ID and password or other authentication item.	Phillip Hagan, QSA# 204-876					
12.3.3 A list of all such devices and personnel with access.			☒	☐	☐	☐	☐
12.3.3 Verify that the usage policies define: ● A list of all critical devices, and ● A list of personnel authorized to use the devices.	**Provide the name of the assessor** who attests that the usage policies were verified to define: ● A list of all critical devices, and ● A list of personnel authorized to use the devices.	Phillip Hagan, QSA# 204-876					
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).			☒	☐	☐	☐	☐
12.3.4 Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).	**Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine: ● Owner ● Contact Information ● Purpose	Phillip Hagan, QSA# 204-876					
12.3.5 Acceptable uses of the technology.			☒	☐	☐	☐	☐
12.3.5 Verify that the usage policies define acceptable uses for the technology.	**Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology.	Phillip Hagan, QSA# 204-876					
12.3.6 Acceptable network locations for the technologies.			☒	☐	☐	☐	☐
12.3.6 Verify that the usage policies define acceptable network locations for the technology.	**Provide the name of the assessor** who attests that the usage policies were verified to define acceptable network locations for the technology.	Phillip Hagan, QSA# 204-876					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.3.7 List of company-approved products.			☒	☐	☐	☐	☐
12.3.7 Verify that the usage policies include a list of company-approved products.	**Provide the name of the assessor** who attests that the usage policies were verified to include a list of company-approved products.	Phillip Hagan, QSA# 204-876					
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.			☒	☐	☐	☐	☐
12.3.8.a Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	**Provide the name of the assessor** who attests that the usage policies were verified to require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	Phillip Hagan, QSA# 204-876					
12.3.8.b Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity.	**Identify** any remote access technologies in use	RDP: High Encryption VPN Client (OpenVPN): TLS 1.2					
	Describe how configurations for remote access technologies verified that remote access sessions will be automatically disconnected after a specific period of inactivity.	360 Advanced inspected system configurations to verify that remote access technologies were configured to automatically disconnect after a specific period of inactivity. RDP sessions were configured to disconnect idle sessions after 15 minutes of inactivity and enforced through Windows Group Policy. Documentation Reviewed: SRV-01.6 Server Remote Management & Idle Timeouts					
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.			☐	☐	☒	☐	☐
12.3.9 Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	**Provide the name of the assessor** who attests that the usage policies were verified to require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	Not Applicable. Fairfax did not provide vendors access to systems within the CDE.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.			☐	☐	☒	☐	☐
12.3.10.a Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	**Provide the name of the assessor** who attests that the usage policies were verified to prohibit copying, moving or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	Not Applicable. Fairfax implemented tokenization of cardholder data and did not store cardholder data within the environment.					
12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	**Provide the name of the assessor** who attests that the usage policies were verified to require, for personnel with proper authorization, the protection of cardholder data in accordance with PCI DSS Requirements.	Not Applicable. Fairfax implemented tokenization of cardholder data and did not store cardholder data within the environment.					
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.			☒	☐	☐	☐	☐
12.4.a Verify that information security policy and procedures clearly define information security responsibilities for all personnel.	**Identify the information security policy and procedures** reviewed to verify that they clearly define information security responsibilities for all personnel.	POL-01 Data Security Policies and Procedures ORG-02 Job Descriptions					
12.4.b Interview a sample of responsible personnel to verify they understand the security policies.	**Identify the responsible personnel** interviewed for this testing procedure who confirm they understand the security policy.	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
12.4.1 ***Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: ● Overall accountability for maintaining PCI DSS compliance ● Defining a charter for a PCI DSS compliance program and communication to executive management			☒	☐	☐	☐	☐
12.4.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance	**Identify the documentation** examined to verify that executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.	ORG-06 PCI DSS Compliance Program & Charter					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.4.1.b Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.	**Identify the company's PCI DSS charter** examined to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.	ORG-06 PCI DSS Compliance Program & Charter					
12.5 Assign to an individual or team the following information security management responsibilities:			☒	☐	☐	☐	☐
12.5 Examine information security policies and procedures to verify: ● The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. ● The following information security responsibilities are specifically and formally assigned:	**Identify the information security policies and procedures** reviewed to verify: ● The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. ● The following information security responsibilities are specifically and formally assigned:	POL-01 Data Security Policies and Procedures					
12.5.1 Establish, document, and distribute security policies and procedures.			☒	☐	☐	☐	☐
12.5.1 Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: ● Establishing security policies and procedures. ● Documenting security policies and procedures. ● Distributing security policies and procedures.	Phillip Hagan, QSA# 204-876					
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.			☒	☐	☐	☐	☐
12.5.2 Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: ● Monitoring and analyzing security alerts. ● Distributing information to appropriate information security and business unit management personnel.	Phillip Hagan, QSA# 204-876					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.			☒	☐	☐	☐	☐
12.5.3 Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: ● Establishing security incident response and escalation procedures. ● Documenting security incident response and escalation procedures. ● Distributing security incident response and escalation procedures.	Phillip Hagan, QSA# 204-876					
12.5.4 Administer user accounts, including additions, deletions, and modifications.			☒	☐	☐	☐	☐
12.5.4 Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for administering user account and authentication management.	Phillip Hagan, QSA# 204-876					
12.5.5 Monitor and control all access to data.			☒	☐	☐	☐	☐
12.5.5 Verify that responsibility for monitoring and controlling all access to data is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: ● Monitoring all access to data ● Controlling all access to data	Phillip Hagan, QSA# 204-876					
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.			☒	☐	☐	☐	☐
12.6.a Review the security awareness program to verify it provides awareness to all personnel about the cardholder data security policy and procedures.	**Provide the name of the assessor** who attests that the security awareness program was verified to provide awareness to all personnel about the cardholder data security policy and procedures.	Phillip Hagan, QSA# 204-876					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.6.b Examine security awareness program procedures and documentation and perform the following:	**Identify the documented security awareness program procedures and additional documentation** examined to verify that: ● The security awareness program provides multiple methods of communicating awareness and educating personnel. ● Personnel attend security awareness training: - Upon hire, and - At least annually ● Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy.	POL-01 Data Security Policies and Procedures ORG-03 Employee Handbook & Code of Conduct SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing) EMP-02.1 Employee Annual Security Awareness Refresher TRN-01 Security Awareness Training Material TRN-02 Developer Secure Coding Training					
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*			☒	☐	☐	☐	☐
12.6.1.a Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions).	**Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel.	360 Advanced inspected the security awareness program to verify that there were multiple methods of communicating awareness and educating personnel. Methods of communication included classroom training, an initial and annual security awareness presentation for new and current employees, and periodic email messages.					
12.6.1.b Verify that personnel attend security awareness training upon hire and at least annually.	**Describe how** it was observed that all personnel attend security awareness training:						
	● Upon hire	360 Advanced inspected signed acknowledgement forms from new employees to verify that all personnel attend security awareness training upon hire. Documentation Reviewed: SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing)					
	● At least annually	360 Advanced inspected completed security awareness refreshers for a sample of active employees within the last year to verify that annual security awareness training was provided at least annually to all employees. Documentation Reviewed: EMP-02.1 Employee Annual Security Awareness Refresher					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.6.1.c Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security.	**Identify the sample** of personnel interviewed for this testing procedure.	New Hire Training: Sample Set-3: New Hires Annual Training: Sample Set-4: Tenured Employees					
	For the interview, **summarize the relevant details** discussed that verify they have completed awareness training and are aware of the importance of cardholder data security.	The sample of personnel interviewed were able to discuss a variety of security and compliance issues, such as the need to protect cardholder data, abiding by password policies, and the use of computers for business purposes only.					
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.			☒	☐	☐	☐	☐
12.6.2 Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.	**Describe how** it was observed that, per the security awareness program, all personnel:						
	● Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic).	360 Advanced inspected electronic policy acknowledgements for a sample of new employees hired within the last year to verify that personnel have read and understood the information security policy upon hire. 360 Advanced noted that policy acknowledgements were incorporated within the security awareness training performed during the onboarding process. Documentation Reviewed: SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing)					
	● Provide an acknowledgement at least annually.	360 Advanced inspected completed security awareness refresher acknowledgements for a sample of active employees within the last year to verify that personnel have read and understood the information security policy on an annual basis. 360 Advanced noted that policy acknowledgements were incorporated within the annual security awareness training refresher. Documentation Reviewed: EMP-02.1 Employee Annual Security Awareness Refresher					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*			☒	☐	☐	☐	☐
12.7 Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	**Identify the Human Resources personnel** interviewed who confirm background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	Maryanne Pearson - Controller					
	Describe how it was observed that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	360 Advanced inquired of responsible personnel and inspected completed background checks to verify that background screens were conducted prior to hiring of potential personnel who would have access to cardholder data or the CDE. The Human Resources personnel described the hiring process, and how an offer is made contingent on a successful background check for all prospective employees. Documentation Reviewed: SOC-00 360 Advanced Testing Sheet - Fairfax - 2021 (See Tab ST-00.1 for New Hire Testing)					
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:			☒	☐	☐	☐	☐
12.8 Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows:	**Identify the documented policies and procedures** reviewed to verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, per 12.8.1–12.8.5:	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.8.1 Maintain a list of service providers including a description of the service provided.			☒	☐	☐	☐	☐
12.8.1 Verify that a list of service providers is maintained and includes a list of the services provided.	**Describe how** the documented list of service providers was observed to be maintained (kept up-to-date) and includes a list of the services provided.	360 Advanced inspected a documented list of current service providers that matched the entities noted during this current assessment. Due diligence conducted, and contractual / written agreements were managed and documented for each service provider. Documentation Reviewed: SP-00 Listing of Third-Party Service Providers					
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's CDE. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*			☒	☐	☐	☐	☐
12.8.2 Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	**Describe how** written agreements for each service provider were observed to include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.	360 Advanced inspected written contracts from a sample of service providers to verify that they included acknowledgement of the responsibility for maintaining all PCI DSS requirements applicable to the services provided by each entity. Documentation Reviewed: SP-00 Listing of Third-Party Service Providers SP-01 Service Provider Contracts & Agreements					
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.			☒	☐	☐	☐	☐
12.8.3 Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider.	**Identify the policies and procedures** reviewed to verify that processes included proper due diligence prior to engaging any service provider.	POL-01 Data Security Policies and Procedures					
	Describe how it was observed that the above policies and procedures are implemented.	360 Advanced noted that Fairfax had not recently engaged in new service provider relationships, but that Fairfax did have policies and procedures in place that specified a due diligence process prior to implementing any new service provider relationships.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.			☒	☐	☐	☐	☐
12.8.4 Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	**Describe how** it was observed that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	360 Advanced inspected the review of third-party audit reports and compliance status for in-scope service providers to verify that a program was maintained to monitor service providers' PCI DSS compliance status at least annually. 360 Advanced noted that this review occurred shortly before the assessment and documented by personnel who reviewed card brand global registry information to verify compliant statuses. Documentation Reviewed: SP-00 Listing of Third-Party Service Providers SP-02 Service Provider Third-Party Auditor Reports					
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.			☒	☐	☐	☐	☐
12.8.5 Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**Describe how** it was observed that the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	360 Advanced inspected third-party audit reports and compliance status for in-scope service providers to verify that information was maintained about which PCI DSS requirements are managed by service providers and which are managed by Fairfax. Documentation Reviewed: SP-00 Listing of Third-Party Service Providers SP-02 Service Provider Third-Party Auditor Reports					
12.9 ***Additional requirement for service providers only:*** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*			☒	☐	☐	☐	☐
12.9 ***Additional testing procedure for service provider assessments only****:* Review service provider's policies and procedures and observe templates used for written agreement to confirm the	**Indicate whether** the assessed entity is a service provider. **(yes/no)** *If "no," mark the remainder of 12.9 as "Not Applicable."* *If "yes":*	Yes.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	**Identify the service provider's policies and procedures** reviewed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	CUS-01 Customer Contracts & Agreements POL-01 Data Security Policies and Procedures					
	Describe how the templates used for written agreement verified that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	360 Advanced inspected the Fairfax Terms of Use and Merchant Service Agreements to verify that Fairfax acknowledges in writing to customers that they will maintain all applicable PCI DSS requirement to the extent they store, process, or transmit cardholder data on behalf of the customer.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.			☒	☐	☐	☐	☐
12.10 Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following:	**Identify the documented incident response plan and related procedures** examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows from 12.10.1–12.10.6: ● Create the incident response plan to be implemented in the event of system breach. ● Test the plan at least annually. ● Designate specific personnel to be available on a 24/7 basis to respond to alerts: ● 24/7 incident monitoring ● 24/7 incident response ● Provide appropriate training to staff with security breach response responsibilities. ● Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. ● Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	AS-04.1 Incident Response Plan AS-04.2 Incident Response Testing & Training POL-01 Data Security Policies and Procedures					
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ● Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. ● Specific incident response procedures. ● Business recovery and continuity procedures. ● Data back-up processes. ● Analysis of legal requirements for reporting compromises. ● Coverage and responses of all critical system components. ● Reference or inclusion of incident response procedures from the payment brands.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.10.1.a Verify that the incident response plan includes: ● Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. ● Specific incident response procedures. ● Business recovery and continuity procedures ● Data back-up processes ● Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). ● Coverage and responses for all critical system components. ● Reference or inclusion of incident response procedures from the payment brands.	**Provide the name of the assessor** who attests that the incident response plan was verified to include: ● Roles and responsibilities. ● Communication strategies. ● Requirement for notification of the payment brands. ● Specific incident response procedures. ● Business recovery and continuity procedures. ● Data back-up processes. ● Analysis of legal requirements for reporting compromises. ● Coverage for all critical system components. ● Responses for all critical system components. ● Reference or inclusion of incident response procedures from the payment brands.	Phillip Hagan, QSA# 204-876					
12.10.1.b Interview personnel and review documentation from a sample of previously reported incidents or alerts to	**Identify the responsible personnel** interviewed who confirm that the documented incident response plan and procedures are followed.	Nadine Chahal - General Counsel					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
verify that the documented incident response plan and procedures were followed.	**Identify the sample** of previously reported incidents or alerts selected for this testing procedure.	There were no incidents that occurred within the past 12 months. However, 360 Advanced observed the alert and ticketing systems to verify that procedures were in place to assess potential incidents and trigger the response plan as appropriate. Documentation Reviewed: AS-04.1 Incident Response Plan AS-04.2 Incident Response Testing & Training POL-01 Data Security Policies and Procedures LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples					
	For each item in the sample, **describe how** the documented incident response plan and procedures were observed to be followed.	360 Advanced inspected an incident response policy and test plan detailing steps to recover from potential failures or malicious attacks on system components and the requirement that the plan be reviewed and tested on annual basis. An incident response form documented the steps throughout the incident response processes including all elements from initial reporting to final resolution and lessons learned. Documentation Reviewed: AS-04.1 Incident Response Plan AS-04.2 Incident Response Testing & Training POL-01 Data Security Policies and Procedures					
12.10.2 Review and test the plan at least annually, including all elements listed in Requirement 12.10.1.			☒	☐	☐	☐	☐
12.10.2 Interview personnel and review documentation from testing to verify that the plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1.	**Identify the responsible personnel** interviewed who confirm that the incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1.	Nadine Chahal - General Counsel					
	Identify documentation reviewed from testing to verify that the incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1.	POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.			☒	☐	☐	☐	☐
12.10.3 Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	**Identify the document** requiring 24/7 incident response and monitoring coverage for: ● Any evidence of unauthorized activity. ● Detection of unauthorized wireless access points. ● Critical IDS alerts. ● Reports of unauthorized critical system or content file changes.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm 24/7 incident response and monitoring coverage for: ● Any evidence of unauthorized activity. ● Detection of unauthorized wireless access points. ● Critical IDS alerts. ● Reports of unauthorized critical system or content file changes.	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					
	Describe how it was observed that designated personnel are available for 24/7 incident response and monitoring coverage for: ● Any evidence of unauthorized activity. ● Detection of unauthorized wireless access points. ● Critical IDS alerts. ● Reports of unauthorized critical system or content file changes.	360 Advanced inspected audit and alert settings to verify that designated personnel were available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, or FIM reporting. Deep Security Manager and AlienVault SIEM were used as repositories and alerting tools for events that evidenced unauthorized activity. Documentation reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples SRV-01.8 Server Audit Settings & Local Log Examples					
12.10.4 Provide appropriate training to staff with security breach response responsibilities.			☒	☐	☐	☐	☐
12.10.4 Verify through observation, review of policies, and interviews of responsible personnel that staff with	**Identify the responsible personnel** interviewed who confirm that staff with responsibilities for security breach response are periodically trained.	Nadine Chahal - General Counsel					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
responsibilities for security breach response are periodically trained.	**Identify the documented policy** reviewed to verify that staff with responsibilities for security breach response are periodically trained.	POL-01 Data Security Policies and Procedures					
	Describe how it was observed that staff with responsibilities for security breach response are periodically trained.	360 Advanced inspected meeting and attendance for an incident response plan interactive roundtable to verify that responsible staff were periodically trained on the security breach response processes. Personnel described how response training was provided by specifically walking through appropriate response steps and communication methods in the event of an incident. Personnel also described how Fairfax integrated breach response training into the annual testing of the incident response plan. Documentation Reviewed: AS-04.2 Incident Response Testing & Training POL-01 Data Security Policies and Procedures					
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.			☒	☐	☐	☐	☐
12.10.5 Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan.	**Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems are covered in the Incident Response Plan.	360 Advanced inspected a sample of log aggregation and alert generations through Deep Security Manager and AlienVault SIEM to verify that alerts from security monitoring systems were being monitored as outlined in the incident response plan. Documentation Reviewed: LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples					
	Describe how processes were reviewed to verify that ***responding to*** alerts from security monitoring systems are covered in the Incident Response Plan.	360 Advanced inspected an incident response policy and incident response plan to verify that processes included the monitoring and responding to alerts from security monitoring systems. Incident response procedures and associated forms documented the steps throughout the incident response processes including all elements from monitoring and alerting of a potential security incident to final resolution and lessons learned. Documentation Reviewed: AS-04.1 Incident Response Plan POL-01 Data Security Policies and Procedures					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			☒	☐	☐	☐	☐
12.10.6 Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan: ● According to lessons learned. ● To incorporate industry developments.	POL-01 Data Security Policies and Procedures					
	Identify the responsible personnel interviewed who confirm that processes are implemented to modify and evolve the incident response plan: ● According to lessons learned. ● To incorporate industry developments.	Nadine Chahal - General Counsel					
	Describe how it was observed that processes are implemented to modify and evolve the incident response plan:						
	● According to lessons learned.	360 Advanced inspected policies and test plans which indicated that lessons learned were incorporated in the ongoing maintenance and updates of the incident response plan.					
	● To incorporate industry developments.	360 Advanced inspected policies and test plans which indicated that industry developments and changes were incorporated in the ongoing maintenance and updates of the incident response plan.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.11 ***Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: ● Daily log reviews ● Firewall rule-set reviews ● Applying configuration standards to new systems ● Responding to security alerts ● Change management processes			☒	☐	☐	☐	☐
12.11.a Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: ● Daily log reviews ● Firewall rule-set reviews ● Applying configuration standards to new systems ● Responding to security alerts ● Change management processes	**Identify the policies and procedures** examined to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: ● Daily log reviews ● Firewall rule-set reviews ● Applying configuration standards to new systems ● Responding to security alerts ● Change management processes	POL-01 Data Security Policies and Procedures					
12.11.b Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly	**Identify the document(s) related to reviews** examined to verify that reviews are performed at least quarterly.	CHG-02 Change Records - System Changes CHG-03 Change Records - Application Changes Deployed to Production LOG-03 Central Log System - Log Settings & Examples LOG-04 Central Log System - Alert Settings & Examples RVW-01 Review of Firewall Rules RVW-03.1 Review of Logical Access for Privileged Users RVW-05 Review of Operational Procedures					
	Identify the responsible personnel interviewed who confirm that reviews are performed at least quarterly	Alex Umansky - Senior Software Engineer Nadine Chahal - General Counsel					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.11.1 ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include: ● Documenting results of the reviews ● Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program			☒	☐	☐	☐	☐
12.11.1.a Examine documentation from the quarterly reviews to verify they include: ● Documenting results of the reviews. ● Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program.	**Identify the document(s) related to quarterly reviews** to verify they include: ● Documenting results of the reviews. ● Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program.	RVW-05 Review of Operational Procedures					

Appendix A: Additional PCI DSS Requirements

This appendix contains additional PCI DSS requirements for different types of entities. The sections within this Appendix include:

- Appendix A1 Additional PCI DSS Requirements for Shared Hosting Providers
- Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI terminal connections
- Appendix A3: Designated Entities Supplemental Validation

Guidance and applicability information is provided within each section.

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

Note: *If the entity is not a shared hosting provider (and the answer at 2.6 was "no," indicate the below as "Not Applicable." Otherwise, complete the below.*

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
Indicate whether the assessed entity is a shared hosting provider (indicated at Requirement 2.6). **(yes/no)** *If "no,"* mark the below as "Not Applicable" (no further explanation required) *If "yes,"* complete the following:		No.					
A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*							
A1 Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A1.1 through A1.4 below:							
A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.			☐	☐	☒	☐	☐
A1.1 If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: ● No entity on the system can use a shared web server user ID.	**Indicate whether** the hosting provider allows hosted entities to run their own applications. **(yes/no)**	No.					
	If "no":						
	Describe how it was observed that hosted entities are not able to run their own applications.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	If "yes":						
	Identify the sample of servers selected for this testing procedure.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
● All CGI scripts used by an entity must be created and run as the entity's unique user ID.	**Identify the sample** of hosted merchants and service providers (hosted entities) selected for this testing procedure.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	For each item in the sample, **describe how** the system configurations verified that all hosted entities' application processes are run using the unique ID of that entity.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	Describe how the hosted entities' application processes were observed to be running using the unique ID of the entity.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
A1.2 Restrict each entity's access and privileges to its own cardholder data environment only.			☐	☐	☒	☐	☐
A1.2.a Verify the user ID of any application process is not a privileged user (root/admin).	*For each item in the sample of servers and hosted entities from A1.1, perform the following:*						
	Describe how the system configurations verified that user IDs for hosted entities' application processes are not privileged users.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	Describe how running application process IDs were observed to verify that the process IDs are not privileged users.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
A1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) ***Important:*** *An entity's files may not be shared by group.*	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** the system configuration settings verified:						
	● Read permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	● Write permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	● Access permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
A1.2.c Verify that an entity's users do not have write access to shared system binaries.	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** the system configuration settings verified that an entity's users do not have write access to shared system binaries.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
A1.2.d Verify that viewing of log entries is restricted to the owning entity.	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** the system configuration settings verified that viewing of log entries is restricted to the owning entity.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	For each item in the sample of servers and hosted entities from A1.1, **describe how** the system configuration settings verified restrictions are in place for the use of:						
	● Disk space	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	● Bandwidth	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	● Memory	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	● CPU	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.			☐	☐	☒	☐	☐
A1.3 Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: ● Logs are enabled for common third-party applications. ● Logs are active by default.	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** processes were observed to verify the following:						
	● Logs are enabled for common third-party applications.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	● Logs are active by default.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
	● Logs are available for review by the owning entity.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Logs are available for review by the owning entity. • Log locations are clearly communicated to the owning entity.	• Log locations are clearly communicated to the owning entity.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					
A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.			☐	☐	☒	☐	☐
A1.4 Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.	**Identify the document** examined to verify that written policies provide for a timely forensics investigation of related servers in the event of a compromise.	Not Applicable. Fairfax offers no services to PCI customers that would classify it as a shared hosting provider.					

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

Entities using SSL and early TLS for POS POI terminal connections must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment terminals. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

The PCI DSS requirements directly affected are:

Requirement 2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
Requirement 2.3	Encrypt all non-console administrative access using strong cryptography.
Requirement 4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

SSL and early TLS must not be used as a security control to meet these requirements, except in the case of POS POI terminal connections as detailed in this appendix. To support entities working to migrate away from SSL/early TLS on POS POI terminals, the following provisions are included:

- New POS POI terminal implementations must not use SSL or early TLS as a security control
- All POS POI terminal service providers must provide a secure service offering**.**
- Service providers supporting existing POS POI terminal implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals in card-present environments that can be verified as not being susceptible to any known exploits for SSL and early TLS, **and the SSL/TLS termination points to which they connect,** may continue using SSL/early TLS as a security control.

This Appendix only applies to entities using SSL/early TLS as a security control to protect POS POI terminals, including service providers who provide connections into POS POI terminals.

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
Indicate whether the assessed entity is using SSL / early TLS for POS POI terminal connections. **(yes/no)** *If "no," mark the below as "Not Applicable" (no further explanation required)* *If "yes,"* ***complete the following (as applicable):***		No.					
A2.1 Where POS POI terminals (at the merchant or payment acceptance location) use SSL and/or early TLS, the entity must confirm the devices are not susceptible to any known exploits for those protocols. ***Note:*** *This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.*			☐	☐	☒	☐	☐
A2.1 *For POS POI terminals using SSL and/or early TLS,* confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	**Identify the documentation** examined to verify that the POS POI terminals using SSL and/or early TLS are not susceptible to any known exploits for SSL/early TLS.	Not Applicable. Fairfax does not deploy devices that capture payment card data via direct physical interaction.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
A2.2 ***Requirement for Service Providers Only:*** All service providers with existing connection points to POS POI terminals referred to in A2.1 that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.			☐	☐	☒	☐	☐
A2.2 Review the documented Risk Mitigation and Migration Plan to verify it includes: ● Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; ● Risk-assessment results and risk-reduction controls in place; ● Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; ● Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; ● Overview of migration project plan to replace SSL/early TLS at a future date.	**Identify the documented Risk Mitigation and Migration Plan** reviewed to verify it includes: ● Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; ● Risk-assessment results and risk-reduction controls in place; ● Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; ● Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; ● Overview of migration project plan to replace SSL/early TLS at a future date.	Not Applicable. Fairfax does not deploy devices that capture payment card data via direct physical interaction.				
A2.3 ***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering.			☐	☐	☒	☐	☐
A2.3 Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for their service.	**Identify the supporting documentation** reviewed to verify the service provider offers a secure protocol option for their service	Not Applicable. Fairfax does not deploy devices that capture payment card data via direct physical interaction.					
	Identify the sample of system components examined for this testing procedure.	Not Applicable. Fairfax does not deploy devices that capture payment card data via direct physical interaction.					
	For each item in the sample, **describe how** system configurations verify that the service provider offers a secure protocol option for their service.	Not Applicable. Fairfax does not deploy devices that capture payment card data via direct physical interaction.					

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities that are required to validate to these requirements should refer to the following documents for reporting:

- *Reporting Template for use with the PCI DSS Designated Entities Supplemental Validation*
- *Supplemental Attestation of Compliance for Onsite Assessments – Designated Entities*

These documents are available in the PCI SSC Document Library.

Note that an entity is ONLY required to undergo an assessment according to this Appendix if instructed to do so by an acquirer or a payment brand.

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Guidance Column* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

   Note: *The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.*

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review.

   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) one-time passwords.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

***Note:** Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

Information Required		Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement noted as being "in place" via compensating controls.

Requirement Number: *8.1.1 – Are all users identified with a unique user ID before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers using their regular user accounts, and then use the "sudo" command to run any administrative commands. This allows use of the "root" account privileges to run pre-defined commands that are recorded by sudo in the security log. In this way, each user's actions can be traced to an individual user account, without the "root" password being shared with the users.*
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the sudo command is configured properly using a "sudoers" file, that only pre-defined commands can be run by specified users, and that all activities performed by those individuals using sudo are logged to identify the individual performing actions using "root" privileges.*
6. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure sudo configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually identified, tracked and logged.*

Appendix D: Segmentation and Sampling of Business Facilities/System Components