Mail Louisville, Inc.

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security (SOC 2, Type II) on the Information Technology General Control Environment System

For the period October 1, 2021 to March 31, 2022

DHG

An Independent Service Auditor Report issued by
Dixon Hughes Goodman LLP

table of contents

section I: independent service auditor's report

To: Management of Mail Louisville, Inc.
Louisville, KY

Scope

We have examined Mail Louisville, Inc.'s ("Mail Louisville") accompanying description of its Information Technology General Control Environment System found in Section III titled "management's description of its system and controls" throughout the period October 1, 2021 to March 31, 2022 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (*AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2021 to March 31, 2022, to provide reasonable assurance that Mail Louisville's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA, *Trust Services Criteria*).

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Mail Louisville, to achieve Mail Louisville's service commitments and system requirements based on the applicable trust services criteria. The description presents Mail Louisville's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Mail Louisville's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Mail Louisville is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Mail Louisville's service commitments and system requirements were achieved. In Section II, Mail Louisville has provided the accompanying assertion titled "management's assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Mail Louisville is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and its assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust

services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section IV, "description of trust services criteria, related controls and results" of this report.

Opinion

In our opinion, in all material respects,

- the description presents Mail Louisville's Information Technology General Control Environment System that was designed and implemented throughout the period October 1, 2021 to March 31, 2022 in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period October 1, 2021 to March 31, 2022 to provide reasonable assurance that Mail Louisville's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the user entities applied the complementary controls assumed in the design of Mail Louisville's controls throughout that period.
- the controls stated in the description operated effectively throughout the period October 1, 2021 to March 31, 2022 to provide reasonable assurance that Mail Louisville's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Mail Louisville's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Mail Louisville; user entities of Mail Louisville's Information Technology General Control Environment System during some or all of the period October 1, 2021 to March 31, 2022; business partners of Mail Louisville subject to risks arising from interactions with the Information Technology General Control Environment System; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

Dixon Hughes Goodman LLP

Greenville, SC
May 17, 2022

section II: management's assertion

We have prepared the accompanying description of Mail Louisville's Information Technology General Control Environment System titled "management's description of its system and controls" throughout the period October 1, 2021 to March 31, 2022 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (*AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Information Technology General Control Environment System that may be useful when assessing the risks arising from interactions with Mail Louisville's system, particularly information about system controls that Mail Louisville has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA, *Trust Services Criteria*).

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Mail Louisville, to achieve Mail Louisville's service commitments and system requirements based on the applicable trust services criteria. The description presents Mail Louisville's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Mail Louisville's controls.

We confirm, to the best of our knowledge and belief, that—

1) The description presents Mail Louisville's Information Technology General Control Environment System that was designed and implemented throughout the period October 1, 2021 to March 31, 2022 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period October 1, 2021 to March 31, 2022 to provide reasonable assurance that Mail Louisville's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the user entities applied the complementary controls assumed in the design of Mail Louisville's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period October 1, 2021 to March 31, 2022 to provide reasonable assurance that Mail Louisville's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Mail Louisville's controls operated effectively throughout that period.

Mail Louisville, Inc.

section III: management's description of its system and controls

Overview of Operations

Mail Louisville, Inc. ("Mail Louisville" or "the Company"), a division of Graphic Village, Cincinnati, Ohio is located in East Louisville, Kentucky. Mail Louisville has been providing Direct Mail Fulfillment across the U.S. since 1995.

Services

- Printing of all types including a 7-color digital press and Perfector Presses for longer runs;
- Packaging with Metallic special effects and digital foil capabilities;
- Die Cutting, Fold, Glue and Tipping;
- Promotional items to build long lasting brand awareness through personalized products;
- Warehousing, Fulfillment & Kitting with Portal-accessed print-on-demand;
- Mailing Services located within a day's drive of 65 percent of North America's population;
- Connect provides a one-stop gateway for ordering all marketing collateral;
- Creative Services to deliver your eye-catching designs through the most effective channels;
- Brand Development helps you develop a unique brand to improve perceptions;
- Marketing Strategy to engage your target audience and grow your business;
- Graphic Design from digital advertising to package design, web design and video;
- Custom Content to tell your story through videos, blogs and social media posts;
- Interactive Marketing array through PURLs, domains, website hosting, social media and SEO; and
- Election solutions to enhance name recognition and inform your voters.

Scope

The scope of this report includes the Information Technology General Control Environment System performed in the Louisville, KY facility for Mail Louisville. In December 2021, Graphic Village announced its acquisition of Mail Louisville. This report does not include the offerings provided by Graphic Village.

The Components of the System Used to Provide the Services

Infrastructure

The following indicates Mail Louisville's general procedure flow of printing operations:

- Data Transmission - Client transmits files via the Internet;
- Validation -Validation ensures the files are received intact and that the client supplies the required processing instructions;
- Processing - Raw data is composed into pages and made ready for printing and/or electronic presentation;

- Printing - Documents are printed and prepared for inserting;
- Inserting - Documents are folded and enclosed in envelopes and prepared for mailing; and
- Mailing - Documents are delivered to the post office.

The Mail Louisville printing operation is an end-to-end system comprising of invoice and statement design and consultation, data transmission, transactional document production, customer service, postal mailing coordination and quality control.

Infrastructure is housed at Mail Louisville's 24,000 S.F. facility located at 12500 Westport Rd, Louisville, KY 40245. Data Specialists manage, cleanse, and certify mail lists using individual networked workstations. The mail lists are then processed through the National Change of Address (NCOA) to update the mailing in the event the recipient has moved during the past two years. Lastly, multiple networked printers are utilized throughout the system to deliver services.

Software

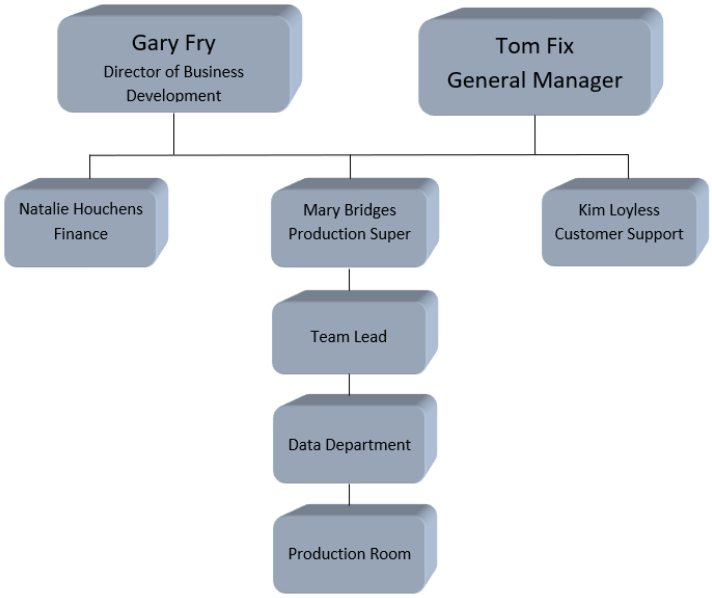
BCC Software, originally Business Computer Center, Inc., is a third party postal and presort software solution. Mail Louisville Data Specialists utilize BCC Software that resides in-house to cleanse and fix addresses provided by clients via incoming file types that include Excel, CSV, XML, TXT, Delimited, etc. The completed address files are then sent to one of multiple printers via an internal PlanetPress License for spooling to a printer. PlanetPress is also an off the shelf software provided by ObjectifLune.

The scope of the report is limited to the BCC and PlanetPress applications.

People

Organizational Structure

The organization is led by the Board of Directors, Chief Executive Officer, and the Chief Financial Officer. Management and direction for the Company originates from this group based on input from the members of senior management, financial partners, and third-party reviews and assessments. The departmental structure divides operations into multiple divisions, including Finance, Sales, Services, and Technology. Managers and staff within each division are assigned responsibility for implementation of corporate policies.



Procedures

Procedures are in place to manage the security of customer data. These processes are documented and address the relevant aspects of the security category of the Trust Services Criteria (TSC) within Mail Louisville's information technology control environment.

Data

The types of data provided by customers is dependent upon the services to be provided. For fulfillment services related to advertising or marketing, clients provide public information for Mail Louisville to process via the Web, email, hard copy, telephone, or fax. Secure transmission methods are used for clients communicating sensitive information that may include client customers' personally identifiable information (PII). Mail Louisville has deployed Secure File Transfer Protocols (SFTP) for the secure transmission of confidential and/or sensitive information over public networks.

Commitments and System Requirements

Commitments

Commitments are declarations made by management to customers within a Master Services Agreement. Commitments are communicated and made publicly available on the Mail Louisville website.

System Requirements

System requirements are specifications regarding how the infrastructure should function to meet the Company's commitments to clients. Requirements are specified in the Company's policies and procedures, which are available to employees.

Relevant Aspects of the Control Environment, Information and Communication, Risk Assessment, and Monitoring

Control Environment

The importance of controls and ethical behavior throughout Mail Louisville is acknowledged by management through implementation of an established control environment that sets the tone for internal activities and processes. Key aspects of the control environment include:

- Integrity and ethical values;
- Commitment to competence;
- Management's philosophy and operating style; and
- Assignment of authority and responsibility.

Integrity and Ethical Values

A Code of Business Conduct and Ethics is reviewed, updated if applicable, and approved by senior management annually. Personnel are required to read and accept the Code of Business Conduct and Ethics upon their hire and

formally reaffirm them annually thereafter. The Code of Business Conduct and Ethics includes a sanctions policy for personnel who violate the documented standards.

Mail Louisville has defined and assigned to appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures. Senior management is responsible for oversight of the organization's Information Security practices and standards. Additionally, departmental meetings are held on a periodic basis to monitor and manage the respective department's progress or lack thereof as it relates to their achievement of the department's responsibilities.

The Company has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets. Purchasing authority designations are documented within Mail Louisville's corporate bylaws.

Commitment to Competence

Prior to employment, Mail Louisville personnel are verified against regulatory screening databases, including at a minimum, criminal (as needed), drug, and employment checks. Before a contractor is onboarded by the Company, the third-party personnel undergo background screening.

Annual performance appraisals are performed with Mail Louisville personnel to evaluate performance in their roles with the Company. Gaps in performance are managed through this process to ensure workforce members are held accountable against organizational standards.

Job requirements are documented in the job descriptions, specifying the responsibilities and skills needed for job positions. Job descriptions are reviewed by management on an annual basis for needed changes. Roles and responsibilities are defined in written job-descriptions.

Management's Philosophy and Operating Style

Mail Louisville operations proceed under direction from senior management who are responsible for maintaining oversight of the organization's control environment.

Assignment of Authority and Responsibility

Reporting relationships and organizational structures are established by senior management as part of organizational planning and adjusted as needed based on changing commitments and requirements. Management has established its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process.

Information and Communication

Mail Louisville has implemented policies and procedures relevant to security to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Organizational policies and procedures are reviewed and updated on at least an annual basis. Any changes to the Company's commitments and system requirements are communicated to internal users. Workforce members are granted access to departmental share drives on the Network where applicable policies and procedures are available.

The Company's security commitments are communicated to newly hired employees to enable them to carry out their responsibilities. Mail Louisville's Acceptable Use Policy addresses personnel requirements for the proper use of Company assets. The policy reinforces management's commitment to protecting Mail Louisville's employees, partners, and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly. Newly onboarded personnel are required to acknowledge their receipt and understanding of the organization's security commitments. Management has also developed in-house trainings describing its security commitments and requirements for personnel to support the achievement of objectives.

The Company's Special Meeting Group meets quarterly to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.

Agreements are established with clients providing sensitive data that include clearly defined terms, conditions, and responsibilities for the Company and clients. Updates or modifications to standard contractual terms and commitments are approved by management prior to contract approval. Contact email addresses and phone numbers are made available on the Company's websites.

Risk Assessment

A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and migration strategies for those risks.

As part of the risk management process, Mail Louisville annually assesses the potential risks and vulnerabilities of the confidentiality, integrity, and availability of critical or confidential information received or processed internally. An IT risk assessment is conducted on Mail Louisville's information system, which includes applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Upon completion of an assessment, the execution, development, and implementation of remediation programs is the joint responsibility of Security Team and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any Risk Assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the Security Team in the development of a remediation plan.

The annual IT risk assessment is used to identify risks arising from both external and internal sources. The risk assessment process includes the following key steps:

- Scope the assessment;
- Gather information;
- Identify threats;
- Identify vulnerabilities;
- Assess security controls;
- Evaluate the potential impact of findings;
- Determine the level of risk;
- Recommend security controls to mitigate identified risks; and

- Document results.

The Company's Special Meeting Group meets quarterly to discuss strategy and operations, and other factors critical to the business. The Special Meeting Group assesses and responds to security risks identified from vulnerability assessments performed and the annual risk assessment.

Cybersecurity insurance is in place to minimize the financial impact of any loss events.

Control Monitoring

Mail Louisville's information security program establishes relevant control activities through oversight of senior management to ensure risks to the control environment are addressed. An Access Control policy is in place to ensure segregation of duties are enforced and privileges are appropriately assigned to users. The Company's policy and procedure manuals are reviewed annually by senior management.

IT strategic planning sessions are held with key members of management to discuss organizational strategies including IT. A course of action is put in place for any potential risks identified within these working sessions that may affect the organization.

Annual PCI vulnerability scans are performed. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities. Additionally, Mail Louisville performs annual risk assessments and communicates results to management for monitoring of corrective actions. Any identified deficiencies are risk rated and evaluated by senior management. The status of deficiencies are monitored until satisfactorily resolved.

Logical and Physical Security

Mail Louisville is headquartered in Louisville, Kentucky. Critical systems utilized for business operations and IT are housed on-site. System components are tracked through an asset inventory listing to log, track, and maintain inventory components.

Logical access to in-scope system components requires a unique username and password (or authorized SSH keys) prior to authenticating users. Passwords for network and in-scope applications are configured according to the Company's policy, which requires an eight-character minimum password length and 90-day password change intervals. Complexity requirements are enabled and enforced through the Active Directory Group Policy and locks users out of the system after five (5) invalid attempts.

A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

Procedures exist for provisioning access to new personnel, changing access, and revoking access to Mail Louisville information systems. Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned. Upon receipt, the Security team will provision the appropriate level of access by assigning a unique user ID and password. The access revocation process begins with the completion of a termination checklist and access is revoked for employees within 24 hours as part of the termination process. Notifications are communicated to appropriate personnel to ensure access to Mail Louisville's systems are removed in a timely manner.

Privileged access to sensitive resources including authentication software is restricted to defined user roles and access to these roles must be approved by the appropriate levels of management. Management performs an annual access review for the in-scope system components to ensure that access is appropriate. Evidence of the annual review is maintained within meeting minutes with the Board of Directors.

Entry and exit points throughout the Mail Louisville facility are physically locked, requiring badge access at times. The badge access system logs user movements throughout the facility. Access to the data centers is reviewed annually by management and documented within the Board of Directors meeting minutes.

Visitors are required to sign in at the front desk prior to proceeding into the facility. Visitors must be escorted to their destination by an authorized employee or their designee.

Formal disposal procedures are in place to guide the secure disposal of the Company's and customers' data. Physical assets and paper media that are no longer needed are destroyed through a third-party destruction company.

Mail Louisville has implemented system firewalls which are configured to limit unnecessary ports, protocols, and services. Host Intrusion detection system is used to provide continuous monitoring of the network and prevention of potential security breaches. The Company has deployed SSH File Transfer Protocol (SFTP) for transmission of confidential and/or sensitive information over public networks.

Mail Louisville has deployed Secure File Transfer Protocols (SFTP) for the secure transmission of confidential and/or sensitive information over public networks. Access to the SFTP server is restricted to the authorized personnel within the organization.

Removable media to be used for customer or system data is required to be encrypted prior to connecting such devices to the information system, in accordance with the Acceptable Use Policy.

Only authorized system administrators are permitted to install software on system devices. Unauthorized use or installation of software is covered in the Code of Business Conduct and Ethical Standards. Local administrator access on end user devices is restricted to appropriate personnel.

Anti-malware technology is deployed within the Mail Louisville environment. This software is used to scan assets prior to being placed into production.

Incident Response and Data Backups

Mail Louisville has implemented an Incident Response Policy to address incidents that may affect the security and integrity of the Company’s information assets, and outlines steps to take in the event of such an incident. Roles and responsibilities have been defined for the Information Security Team who are responsible for navigating the through a security incident from the initial investigation to mitigation, to post incident review.

When an incident is suspected or occurs the Information Security Team is notified, and the incident is documented in a Security Incident Log which contains a summary of completed and on-going security incidents and the organization’s response to that incident. Once an incident has been reported it is the responsibility of the Information Security Team to determine the level of intervention required and whether the incident is electronic or physical.

An Incident Summary Report is completed and documented by the Information Security Team at the conclusion of a security incident. This report provides a detailed summary of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. The Incident Summary Report is used evaluate the procedures of the Security Incident Response Policy, including how the Information Security Team followed the procedures and whether updates are required.

Mail Louisville classifies incidents into two (2) categories:

1. Physical

2. Electronic

After the conclusion of the incident a compiled Incident Report is presented by the Information Security Team to management to discuss the event in detail, review response procedures and construct a Process Improvement Plan to prevent a reoccurrence of that or similar incidents.

To restore data in the event of a security incident, data backups are configured for in-scope applications.

Changes to the System

Mail Louisville recognizes the importance of change management and the associated risks with ineffective change control processes and has documented the Change Management and Control Policy to address the opportunities and associated risks. The change control process is defined and documented within Mail Louisville policies.

The change control process should include the following phases:

- Logged change requests;
- Identification, prioritization, and initiation of change;
- Proper authorization of change;
- Inter-dependency and compliance analysis;
- Impact assessment;
- Change approach;
- Change testing (as applicable);
- User acceptance testing and approval (as applicable);
- Implementation and release planning;
- Change monitoring; and
- Emergency change classification parameters.

Change requests are required to be logged whether approved or rejected. The approval of change requests and the results thereof are documented.

An audit trail is maintained at a Business Unit Level which contains relevant information of the implemented change. This includes change request documentation, change authorization and the outcome of the change. No single person can effect changes to production information systems without the approval of authorized personnel.

Change requests are categorized in terms of benefits, urgency, effort required and potential impact on operations.

As applicable, changes are tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security, and to verify that only intended and approved changes were made.

Specific procedures to ensure the proper control, authorization, and documentation of emergency changes are in place.

Additional Information about Management's Description

Applicable Trust Services Criteria and related controls are included within Section IV of this report, "description of trust services criteria, related controls, and results". Although the applicable Trust Services Criteria and related controls are presented within Section IV, they are, nevertheless, an integral part of the Company's description of its system as described within this section.

Complementary User Entity Controls

Mail Louisville's processes were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain criteria included in this report. This section describes additional internal controls that should be in operation at user organizations to complement internal controls. The complementary user entity controls below do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

Complementary User Entity Controls (CUECs)	Related Criteria
General Information Security Controls	
User organizations are responsible for performing annual user access reviews to Mail Louisville's SFTP portal.	CC 6.2 CC 6.3
User organizations are responsible for confirming access to the Mail Louisville services is immediately disabled for terminated user entity personnel.	CC 6.2 CC 6.3
User organizations are responsible for changing passwords to Mail Louisville's SFTP portal periodically – at least every 90 days.	CC 6.1
User organizations are responsible for deleting their personal data from Mail Louisville resources when necessary.	CC 6.5
User organizations are responsible for notifying Mail Louisville of any issues, problems, or needed changes.	CC 8.1

section IV: description of trust services criteria, related controls, and results

A. INFORMATION PROVIDED BY DIXON HUGHES GOODMAN LLP

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the Specified Period, those prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Company;
- How the Company's System interacts with user entities, subservice organizations, or other parties;
- Internal control and its limitations;
- Complementary user entity controls and how they interact with related controls at the Company to meet the Applicable Trust Services Criteria;
- The Applicable Trust Services Criteria; and
- The risks that may threaten the achievement of the Applicable Trust Services Criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties. This report, when combined with an understanding of the user control considerations in place at user locations, is intended to assist user organizations in assessing control risks.

The scope of our testing of the Company's controls was limited to the controls specified by the Company contained in Section IV of this report. Management believes these are the relevant key controls for the stated criteria. Other than specifically identified controls related to subservice organizations as described in Sections III and IV, our review was not extended to controls in effect at the user organizations, subservice organizations, or third-party vendors.

B. TYPES AND DESCRIPTION OF THE TESTS OF OPERATING EFFECTIVENESS

Various testing methods are used to assess the operating effectiveness of controls during the Specified Period. The table below describes the various methods which were employed in testing the operating effectiveness of controls that are in place at the Company.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control

C. TRUST SERVICES CRITERIA, CONTROLS, TESTS PERFORMED AND RESULTS OF TESTING

The following matrices describe the Company's controls and the testing performed to determine whether the Company's controls were suitably designed and were operating effectively throughout the period to meet the criteria.

Inapplicable Criteria

The following criteria were judged out of scope during our examination due to the non-applicability to the description of the system or the scope of services offered by Mail Louisville:

CC 1.0 Common Criteria Related to Control Environment		
Criteria Number	**Inapplicable Criteria**	**Reason that Criteria is Inapplicable to the Service Organization**
1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Mail Louisville is a third-party direct mail fulfillment service provider to user organizations with senior management consisting of the President and Vice President. Due to the size, complexity, and organizational structure, this criterion does not apply.
CC 9.0 Common Criteria Related to Risk Mitigation		
Criteria Number	**Inapplicable Criteria**	**Reason that Criteria is Inapplicable to the Service Organization**
9.2	The entity assesses and manages risks associated with vendors and business partners.	Mail Louisville does not outsource any key business processes to subservice organizations and as such, this criterion does not apply.

Criteria Group 1: Common Criteria Related to Control Environment

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1	**The entity demonstrates a commitment to integrity and ethical values.**		
1.1.1	A Code of Business Conduct and Ethics is reviewed, updated if applicable, and approved by senior management annually.	Inspected the Code of Business Conduct and Ethics to determine that a Code of Business Conduct and Ethics was reviewed, updated if applicable, and approved by senior management within the year.	No exceptions noted.
1.1.2	Personnel are required to read and accept the Code of Business Conduct and Ethics upon their hire and formally reaffirm them annually thereafter.	Inspected the signed Code of Business Conduct and Ethics related to a sample of new hires to determine that personnel were required to read and accept the Code of Business Conduct and Ethics upon their hire.	There were no instances of a new hire during the period; therefore, the control did not operate during the period.
		Inspected the signed Code of Business Conduct and Ethics related to a sample of employees to determine that personnel were required to read and accept the Code of Business Conduct and Ethics within the year.	No exceptions noted.
1.1.3	The Code of Business Conduct and Ethics includes a sanctions policy for personnel who violate the Code of Business Conduct and Ethics.	Inspected the Code of Business Conduct and Ethics to determine that the Code of Business Conduct and Ethics included a sanctions policy for personnel who violate the Code of Business Conduct and Ethics.	No exceptions noted.
1.1.4	Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks.	Inspected the background checks related to a sample of new hires to determine that personnel were verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks prior to employment.	There were no instances of a new hire during the period; therefore, the control did not operate during the period.

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1	**The entity demonstrates a commitment to integrity and ethical values.**		
1.1.5	Before a contractor is onboarded by the Company, the third-party personnel undergo background screening. Requirements for background checks to be performed by the staffing agency are outlined in contractual agreements.	Inspected the background checks related to a sample of new contractors to determine that the third-party personnel completed a background screening prior to onboarding with the Company.	There were no instances of a new contractor during the period; therefore, the control did not operate during the period.
		Inspected the signed contractual agreement in place with the staffing agency to determine that requirements for background checks were required to be completed prior to onboarding with the Company.	No exceptions noted.
CC 1.3	**Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**		
1.3.1	Management has established its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process.	Inspected the organizational chart to determine that management established its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process.	No exceptions noted.
1.3.2	Job descriptions are reviewed by management on an annual basis for needed changes.	Inspected the annual performance and job description reviews related to a sample of employees to determine that job descriptions were reviewed by management for needed changes within the year.	No exceptions noted.

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.3	**Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**		
1.3.3	Roles and responsibilities are defined in written job descriptions. Reporting relationships and organizational structures are established by senior management as part of organizational planning and adjusted as needed based on changing commitments and requirements.	Inspected the job descriptions related to a sample of employees to determine that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
		Inspected the organizational chart to determine that reporting relationships and organizational structures were established by senior management as part of organizational planning and adjusted as needed based on changing commitments and requirements.	
1.3.4	The confidentiality commitments and obligations of user entities (clients) providing sensitive data to the Company are included in standard services agreements.	Inspected the signed services agreements related to a sample of clients to determine that the confidentiality commitments and obligations of user entities (clients) providing sensitive data to the Company were included in standard services agreements.	No exceptions noted.
CC 1.4	**The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**		
1.4.1	Job requirements are documented in the job descriptions, specifying the responsibilities and skills needed for job positions.	Inspected the job descriptions related to a sample of employees to determine that job requirements were documented in the job descriptions, specifying the responsibilities and skills needed for job positions.	No exceptions noted.
1.4.2	Annual performance appraisals are performed with Mail Louisville personnel to evaluate performance in their roles with the Company.	Inspected the annual performance and job description reviews related to a sample of employees to determine that annual performance appraisals were performed with Mail Louisville personnel to evaluate performance in their roles with the Company within the year.	No exceptions noted.

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.4	**The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**		
1.4.3	Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks.	Inspected the background checks related to a sample of new hires to determine that personnel were verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks prior to employment.	There were no instances of a new hire during the period; therefore, the control did not operate during the period.
CC 1.5	**The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**		
1.5.1	Mail Louisville has defined and assigned to appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures.	Inspected the Security Policy to determine that Mail Louisville defined and assigned to appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures.	No exceptions noted.
1.5.2	Management has assigned responsibilities for implementation of the entity's Information Security policies to the President.	Inspected the corporate bylaws to determine that management assigned responsibilities for implementation of the entity's Information Security policies to the President.	No exceptions noted.

Criteria Group 2: Common Criteria Related to Information and Communication

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1	**The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**		
2.1.1	An IT risk assessment is performed at least annually to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	No exceptions noted.
2.1.2	An IT risk assessment is performed at least annually to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	No exceptions noted.
2.1.3	Policies and procedures relevant to security have been implemented to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.	Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that policies and procedures relevant to security have been implemented to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.	No exceptions noted.
CC 2.2	**The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**		
2.2.1	Internal personnel are granted access to departmental share drives on the Network where applicable policies and procedures are available.	Inspected the internal Network share drives to determine that internal personnel were granted access to departmental share drives on the Network where applicable policies and procedures were available.	No exceptions noted.

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2	**The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**		
2.2.2	The Company's Special Meeting Group meets quarterly to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.	Inspected the quarterly Special Meeting Group minutes related to a sample of quarters to determine that the Company's Special Meeting Group met quarterly to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.	No exceptions noted.
2.2.3	Internal users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the internal Network share drives and the Incident Response Policy and Incident Response Form to determine that internal users were provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
2.2.4	The Company's security commitments are communicated to newly hired employees to enable them to carry out their responsibilities.	Inspected the onboarding packets and signed policies related to a sample of new hires to determine that the Company's security commitments were communicated to newly hired employees to enable them to carry out their responsibilities.	There were no instances of a new hire during the period; therefore, the control did not operate during the period.
2.2.5	Management has developed in-house trainings describing its security commitments and requirements for personnel to support the achievement of objectives.	Inspected the in-house training attendance sheet to determine that management developed in-house trainings describing its security commitments and requirements for personnel to support the achievement of objectives.	No exceptions noted.

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2	**The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**		
2.2.6	Changes to the Company's commitments and system requirements are communicated to internal users.	Inspected the internal Network share drives to determine that changes to the Company's policies and procedures were communicated to internal users on the share drives on the Network.	No exceptions noted.
		Inspected email communications to personnel to determine that changes to the Company's commitments and system requirements were communicated to internal users.	There were no instances of a commitment or system requirement change during the period; therefore, the control did not operate during the period.
2.2.7	Policies and procedures are in place detailing personnel requirements for the proper use of Company assets.	Inspected the Acceptable Use Policy to determine that policies and procedures were in place detailing personnel requirements for the proper use of Company assets.	No exceptions noted.
2.2.8	Policies and procedures are reviewed and updated no less than annually.	Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that policies and procedures were reviewed and updated within the year.	No exceptions noted.

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.3	**The entity communicates with external parties regarding matters affecting the functioning of internal control.**		
2.3.1	Service agreements are established with clients providing sensitive data that include clearly defined terms, conditions, and responsibilities for the Company and clients.	Inspected the signed services agreements related to a sample of clients to determine that service agreements were established with clients providing sensitive data that include clearly defined terms, conditions, and responsibilities for the Company and clients.	No exceptions noted.
2.3.2	Incident response policies and procedures are in place that include an escalation plan based on the nature and severity of the incident.	Inspected the Incident Response Policy and Incident Response Form to determine that incident response policies and procedures were in place that include an escalation plan based on the nature and severity of the incident.	No exceptions noted.
2.3.3	Contact email addresses and phone numbers are made available on the Company's website.	Inspected the public-facing Mail Louisville website to determine that contact email addresses and phone numbers were made available on the Company's website.	No exceptions noted.

Criteria Group 3: Common Criteria Related to Risk Assessment

CC 3.0 Common Criteria Related to Risk Assessment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.1	**The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**		
3.1.1	An IT risk assessment is performed at least annually to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	No exceptions noted.
3.1.2	An IT risk assessment is performed at least annually to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	No exceptions noted.
CC 3.2	**The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**		
3.2.1	The Company's Special Meeting Group meets quarterly to discuss strategy and operations, and other factors critical to the business.	Inspected the quarterly Special Meeting Group minutes related to a sample of quarters to determine that the Company's Special Meeting Group met quarterly to discuss strategy and operations, and other factors critical to the business.	No exceptions noted.
3.2.2	An annual IT risk assessment is performed to identify risks arising from external and internal sources.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify risks arising from external and internal sources.	No exceptions noted.

CC 3.0 Common Criteria Related to Risk Assessment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.2	**The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**		
3.2.3	The Special Meeting Group assesses and responds to security risks on an ongoing basis through regular meetings with IT personnel, performing vulnerability assessments, and conducting a formal annual IT risk assessment.	Inspected the quarterly Special Meeting Group minutes related to a sample of quarters to determine that the Special Meeting Group assessed and responded to security risks on a quarterly basis through regular meetings with IT personnel, performing vulnerability assessments, and conducting a formal annual IT risk assessment.	No exceptions noted.
3.2.4	The Company has a defined information classification scheme for the labeling and handling of data. The Company classifies data into three levels: confidential, sensitive, and public.	Inspected the Data Classification Policy to determine whether that the Company defined an information classification scheme for the labeling and handling of data, and that the Company classified data into three levels: confidential, sensitive, and public.	No exceptions noted.
CC 3.3	**The entity considers the potential for fraud in assessing risks to the achievement of objectives.**		
3.3.1	The Company has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	Inspected the Shareholders' Agreement, Acceptable Use Policy, and the Media Disposal Policy to determine that the Company established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	No exceptions noted.
CC 3.4	**The entity identifies and assesses changes that could significantly impact the system of internal control.**		
3.4.1	The Company's Special Meeting Group meets quarterly to discuss strategy and operations, and other factors critical to the business.	Inspected the quarterly Special Meeting Group minutes related to a sample of quarters to determine that the Company's Special Meeting Group met quarterly to discuss strategy and operations, and other factors critical to the business.	No exceptions noted.

CC 3.0 Common Criteria Related to Risk Assessment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.4	**The entity identifies and assesses changes that could significantly impact the system of internal control.**		
3.4.2	An IT risk assessment is performed at least annually to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	No exceptions noted.

Criteria Group 4: Common Criteria Related to Monitoring Activities

CC 4.0 Common Criteria Related to Monitoring Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.1	**The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**		
4.1.1	Management performs an annual IT risk assessment and communicates results to management for monitoring of corrective actions.	Inspected the annual risk assessment documentation to determine that management performed an IT risk assessment within the year and communicated results to management for monitoring of corrective actions.	No exceptions noted.
4.1.2	Annual PCI vulnerability scans are performed. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum.	Inspected the most recent PCI vulnerability scanning results to determine that PCI vulnerability scans were performed within the year.	No exceptions noted.
		Inspected the remediation plan and tracking documentation to determine that a remediation plan was developed, and changes were implemented to remediate critical and high vulnerabilities at a minimum.	There were no instances of a critical or high vulnerability identified during the period; therefore, the control did not operate during the period.
CC 4.2	**The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective actions, including senior management and the Board of Directors, as appropriate.**		
4.2.1	Management performs an annual IT risk assessment and communicates results to management for monitoring of corrective actions.	Inspected the annual risk assessment documentation to determine that management performed an IT risk assessment within the year and communicated results to management for monitoring of corrective actions.	No exceptions noted.

CC 4.0 Common Criteria Related to Monitoring Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.2	**The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective actions, including senior management and the Board of Directors, as appropriate.**		
4.2.2	The Special Meeting Group assesses and responds to security risks on an ongoing basis through regular meetings with IT personnel, performing vulnerability assessments, and conducting a formal annual IT risk assessment.	Inspected the quarterly Special Meeting Group minutes related to a sample of quarters to determine that the Special Meeting Group assessed and responded to security risks on a quarterly basis through regular meetings with IT personnel, performing vulnerability assessments, and conducting a formal annual IT risk assessment.	No exceptions noted.
4.2.3	Management tracks the status of all deficiencies until satisfactorily resolved.	Inspected the quarterly Special Meeting Group minutes related to a sample of quarters and the annual IT risk assessment documentation to determine that management tracked the status of all deficiencies until satisfactorily resolved.	No exceptions noted.

Criteria Group 5: Common Criteria Related to Control Activities

CC 5.0 Common Criteria Related to Control Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1	**The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**		
5.1.1	An IT risk assessment is performed at least annually to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	No exceptions noted.
5.1.2	Management has assigned responsibilities for implementation of the entity's Information Security policies to the President.	Inspected the corporate bylaws to determine that management assigned responsibilities for implementation of the entity's Information Security policies to the President.	No exceptions noted.
5.1.3	The Special Meeting Group assesses and responds to security risks on an ongoing basis through regular meetings with IT personnel, performing vulnerability assessments, and conducting a formal annual IT risk assessment.	Inspected the quarterly Special Meeting Group minutes related to a sample of quarters to determine that the Special Meeting Group assessed and responded to security risks on a quarterly basis through regular meetings with IT personnel, performing vulnerability assessments, and conducting a formal annual IT risk assessment.	No exceptions noted.
CC 5.2	**The entity also selects and develops general control activities over technology to support the achievement of objectives.**		
5.2.1	An IT risk assessment is performed at least annually to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	No exceptions noted.

CC 5.0 Common Criteria Related to Control Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.2	**The entity also selects and develops general control activities over technology to support the achievement of objectives.**		
5.2.2	An IT risk assessment is performed at least annually to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	No exceptions noted.
CC 5.3	**The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**		
5.3.1	Policies and procedures relevant to security have been implemented to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.	Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that policies and procedures relevant to security have been implemented to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.	No exceptions noted.
5.3.2	Mail Louisville has defined and assigned to appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures.	Inspected the Security Policy to determine that Mail Louisville defined and assigned to appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures.	No exceptions noted.
5.3.3	Policies and procedures are reviewed and updated no less than annually.	Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that policies and procedures were reviewed and updated within the year.	No exceptions noted.

Criteria Group 6: Common Criteria Related to Logical and Physical Access Controls

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1	**The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**		
6.1.1	System components are tracked through an asset inventory listing to log, track, and maintain inventory components.	Inspected the asset inventory listing to determine that system components were tracked through an asset inventory listing to log, track, and maintain inventory components.	No exceptions noted.
6.1.2	In-scope system components require unique username and passwords (or authorized Secure Shell (SSH) keys) prior to authenticating users.	Inspected the network, BCC, and PlanetPress user listings and password configurations to determine that the in-scope system components required unique username and passwords (or authorized Secure Shell (SSH) keys) prior to authenticating users.	No exceptions noted.
6.1.3	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately.	Inspected the most recent access review documentation for the network, BCC, and PlanetPress to determine that access reviews were performed within the year for the in-scope system components to ensure that access was restricted appropriately.	No exceptions noted.
6.1.4	The Company has a defined information classification scheme for the labeling and handling of data. The Company classifies data into three levels: confidential, sensitive, and public.	Inspected the Data Classification Policy to determine whether that the Company defined an information classification scheme for the labeling and handling of data, and that the Company classified data into three levels: confidential, sensitive, and public.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1	**The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**		
6.1.5	Passwords for the network are configured according to the Company's policy, which (a) requires eight character minimum and 90-day password changes; (b) is complexity enabled; and (c) locks users out of the system after five invalid attempts.	Compared the network domain password configurations to the Password Policy to determine that passwords for the network were configured according to the Company's policy, which (a) requires eight character minimum and 90-day password changes; (b) is complexity enabled; and (c) locks users out of the system after five invalid attempts.	No exceptions noted.
6.1.6	Passwords for in-scope system components are configured according to the Company's policy, which (a) requires eight-character minimum and 90-day password changes; (b) is complexity enabled; and (c) locks users out of the system after five invalid attempts.	Compared the BCC and PlanetPress password configurations to the Password Policy to determine that passwords for the in-scope system components were configured according to the Company's policy, which (a) requires eight character minimum and 90-day password changes; (b) is complexity enabled; and (c) locks users out of the system after five invalid attempts.	No exceptions noted.
6.1.7	The Change Management and Control Policy requires that system changes undergo formal documentation, review, and authorization.	Inspected the Change Management and Control Policy to determine that the Change Management and Control Policy required that system changes undergo formal documentation, review, and authorization.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.2	**Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.**		
6.2.1	Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request forms related to a sample of new hires to determine that access to in-scope system components required a documented access request form and manager approval prior to access being provisioned.	There were no instances of a new hire during the period; therefore, the control did not operate during the period.
6.2.2	A termination checklist is completed, and access is revoked for employees within 24 hours as part of the termination process.	Inspected the termination checklists related to a sample of terminations to determine that a termination checklist was completed, and that access was revoked for employees within 24 hours as part of the termination process.	There were no instances of a termination during the period; therefore, the control did not operate during the period.
		Inspected the network, BCC, and PlanetPress user listings to determine that access related to a sample of terminations was revoked within 24 hours as part of the termination process.	
6.2.3	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately.	Inspected the most recent access review documentation for the network, BCC, and PlanetPress to determine that access reviews were performed within the year for the in-scope system components to ensure that access was restricted appropriately.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.3	**The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.**		
6.3.1	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately.	Inspected the most recent access review documentation for the network, BCC, and PlanetPress to determine that access reviews were performed within the year for the in-scope system components to ensure that access was restricted appropriately.	No exceptions noted.
6.3.2	A termination checklist is completed, and access is revoked for employees within 24 hours as part of the termination process.	Inspected the termination checklists related to a sample of terminations to determine that a termination checklist was completed, and that access was revoked for employees within 24 hours as part of the termination process. Inspected the network, BCC, and PlanetPress user listings to determine that access related to a sample of terminations was revoked within 24 hours as part of the termination process.	There were no instances of a termination during the period; therefore, the control did not operate during the period.
6.3.3	Administrative access to in-scope systems and the network is restricted to appropriate individuals to support segregation of duties.	Inspected the network, BCC, and PlanetPress administrator user listings and inquired of management to determine that administrative access to in-scope systems and the network was restricted to appropriate individuals to support segregation of duties.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.4	**The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**		
6.4.1	Doors to the Mail Louisville facility are physically locked, requiring badge access at all times. Visitors must call for assistance to be granted access.	Inspected evidence of badge readers and locked doors at the Mail Louisville facility to determine that doors to the Mail Louisville facility were physically locked, requiring badge access at all times, and that visitors must call for assistance to be granted access.	No exceptions noted.
6.4.2	A termination checklist is completed, and physical access is revoked for employees within 24 hours as part of the termination process.	Inspected the termination checklists related to a sample of terminations to determine that a termination checklist was completed, and that physical access was revoked for employees within 24 hours as part of the termination process. Inspected the facility badge user listing to determine that physical access related to a sample of terminations was revoked within 24 hours as part of the termination process.	There were no instances of a termination during the period; therefore, the control did not operate during the period.
6.4.3	Visitors are required to sign-in at the front desk prior to proceeding into the facility. All visitors must be escorted to their destination by an authorized employee or their designee.	Inspected the visitor sign-in logs to determine that visitors were required to sign-in at the front desk prior to proceeding into the facility. Inquired of management to determine that all visitors must be escorted to their destination by an authorized employee or their designee.	No exceptions noted.
6.4.4	Access to the data center is reviewed annually by management and documented within the Board of Directors meeting minutes.	Inspected the most recent access review documentation for the data center to determine that access to the data center was performed within the year by management and documented within the Board of Directors meeting minutes.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.4	**The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**		
6.4.5	Badge and access key card are required to access entry points at the Company's facilities and computer rooms. Key card activity is logged and maintained.	Inspected evidence of badge readers and locked doors at the Mail Louisville facility to determine that badge and access key card were required to access entry points at the Company's facilities and computer rooms	No exceptions noted.
		Inspected the badge and key card audit logs and system configurations to determine that key card activity was logged and maintained.	
CC 6.5	**The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.**		
6.5.1	Disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the Data Retention Policy to determine that disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
6.5.2	Physical assets and paper media that are no longer needed are destroyed through a third-party destruction company.	Inspected the certificates of destruction related to a sample of destroyed physical assets and paper media to determine that physical assets and paper media that were no longer needed were destroyed through a third-party destruction company.	No exceptions noted.
CC 6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**		
6.6.1	System firewalls are configured to limit unnecessary ports, protocols, and services.	Inspected the firewall configurations and rulesets to determine that system firewalls were configured to limit unnecessary ports, protocols, and services.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**		
6.6.2	The Company has deployed Secure Shell (SSH) File Transfer Protocol (SFTP) for transmission of confidential and/or sensitive information over public networks.	Inspected the SFTP encryption configurations to determine that the Company deployed Secure Shell (SSH) File Transfer Protocol (SFTP) for transmission of confidential and/or sensitive information over public networks.	No exceptions noted.
6.6.3	An Intrusion Detection System (IDS) is used to provide continuous monitoring of the network and prevention of potential security breaches.	Inspected the IDS configurations and alert settings to determine that an Intrusion Detection System (IDS) was used to provide continuous monitoring of the network and prevention of potential security breaches.	No exceptions noted.
CC 6.7	**The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.**		
6.7.1	Access to the SFTP server is restricted to the data specialists' group.	Inspected the SFTP server user listing and inquired of management to determine that access to the SFTP server was restricted to the data specialists' group.	No exceptions noted.
6.7.2	The Company has deployed Secure Shell (SSH) File Transfer Protocol (SFTP) for transmission of confidential and/or sensitive information over public networks.	Inspected the SFTP encryption configurations to determine that the Company deployed Secure Shell (SSH) File Transfer Protocol (SFTP) for transmission of confidential and/or sensitive information over public networks.	No exceptions noted.
6.7.3	Removable media to be used for customer or system data is required to be encrypted prior to connecting such devices to the information system, in accordance with the Acceptable Use Policy.	Inspected the group policy object configurations and the Acceptable Use Policy to determine that removable media to be used for customer or system data was required to be encrypted prior to connecting such devices to the information system, in accordance with the Acceptable Use Policy.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**		
6.8.1	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software is explicitly covered in the Code of Business Conduct and Ethics.	Inspected the listing of local system administrators and inquired of management to determine that only authorized system administrators were able to install software on system devices. Inspected the Code of Business Conduct and Ethics to determine that unauthorized use or installation of software was explicitly covered in the Code of Business Conduct and Ethics.	No exceptions noted.
6.8.2	Local administrator access on end user devices is restricted to appropriate personnel.	Inspected the listing of local system administrators and inquired of management to determine that local administrator access on end user devices was restricted to appropriate personnel.	No exceptions noted.
6.8.3	Change management procedures are in place to govern the modification of critical company information resources and address security requirements.	Inspected the Change Management and Control Policy to determine that change management procedures were in place to govern the modification of critical company information resources and address security requirements.	No exceptions noted.
6.8.4	Anti-malware technology is deployed for environments. The anti-malware software is configured to automatically scan and update regularly.	Inspected the anti-malware and anti-virus scanning and update configurations to determine that anti-malware technology was deployed for environments, and that the anti-malware software was configured to automatically scan and update regularly.	No exceptions noted.

Criteria Group 7: Common Criteria Related to System Operations

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.1	**To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**		
7.1.1	Baseline security configurations are evaluated on an annual basis to ensure any potential vulnerabilities are identified.	Inspected the most recent PCI vulnerability scanning results to determine that baseline security configurations were evaluated within the year to ensure any potential vulnerabilities are identified.	No exceptions noted.
7.1.2	Annual PCI vulnerability scans are performed. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum.	Inspected the most recent PCI vulnerability scanning results to determine that PCI vulnerability scans were performed within the year. Inspected the remediation plan and tracking documentation to determine that a remediation plan was developed, and changes were implemented to remediate critical and high vulnerabilities at a minimum.	No exceptions noted.
CC 7.2	**The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.**		
7.2.1	Contact email addresses and phone numbers are made available on the Company's website.	Inspected the public-facing Mail Louisville website to determine that contact email addresses and phone numbers were made available on the Company's website.	No exceptions noted.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.2	**The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.**		
7.2.2	When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.	Inspected the Incident Response Policy and Incident Response Form to determine that when a potential security incident is detected, a defined incident management process should be initiated by authorized personnel.	No exceptions noted.
		Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that a defined incident management process was initiated by authorized personnel, and that corrective actions were implemented in accordance with defined policies and procedures.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.
7.2.3	An Intrusion Detection System (IDS) is used to provide continuous monitoring of the network and prevention of potential security breaches.	Inspected the IDS configurations and alert settings to determine that an Intrusion Detection System (IDS) was used to provide continuous monitoring of the network and prevention of potential security breaches.	No exceptions noted.
7.2.4	Incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that incidents related to security were logged, tracked, and communicated to affected parties by management until resolved.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.2	**The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.**		
7.2.5	An IT risk assessment is performed at least annually to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements related to security.	No exceptions noted.
CC 7.3	**The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**		
7.3.1	Internal users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the internal Network share drives and the Incident Response Policy and Incident Response Form to determine that internal users were provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
7.3.2	Incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that incidents related to security were logged, tracked, and communicated to affected parties by management until resolved.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3	**The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**		
7.3.3	Security incidents are analyzed including what specific attack occurred, which system(s) were affected and what happened during the attack. A root cause analysis is performed to determine the classification and impact of the event.	Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that security incidents were analyzed including what specific attack occurred, which system(s) were affected and what happened during the attack, and that a root cause analysis was performed to determine the classification and impact of the event.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.
CC 7.4	**The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**		
7.4.1	Mail Louisville has defined and assigned to appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures.	Inspected the Security Policy and Incident Response Policy to determine that Mail Louisville defined and assigned to appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures.	No exceptions noted.
7.4.2	When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.	Inspected the Incident Response Policy and Incident Response Form to determine that when a potential security incident is detected, a defined incident management process should be initiated by authorized personnel.	No exceptions noted.
		Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that a defined incident management process was initiated by authorized personnel, and that corrective actions were implemented in accordance with defined policies and procedures.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4	**The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**		
7.4.3	Real-time incremental and daily full backups are configured for the network and in-scope system components.	Inspected the backup configurations to determine that real-time incremental and daily full backups were configured for the network and in-scope system components.	No exceptions noted.
7.4.4	Incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that incidents related to security were logged, tracked, and communicated to affected parties by management until resolved.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.
7.4.5	Annual PCI vulnerability scans are performed. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum.	Inspected the most recent PCI vulnerability scanning results to determine that PCI vulnerability scans were performed within the year. Inspected the remediation plan and tracking documentation to determine that a remediation plan was developed, and changes were implemented to remediate critical and high vulnerabilities at a minimum.	No exceptions noted.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
7.5.1	Incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that incidents related to security were logged, tracked, and communicated to affected parties by management until resolved.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.
7..5.2	Security incidents are analyzed including what specific attack occurred, which system(s) were affected and what happened during the attack. A root cause analysis is performed to determine the classification and impact of the event.	Inspected the security incident tickets and reporting documentation related to a sample of security incidents to determine that security incidents were analyzed including what specific attack occurred, which system(s) were affected and what happened during the attack, and that a root cause analysis was performed to determine the classification and impact of the event.	There were no instances of a confirmed security incident or breach during the period; therefore, the control did not operate during the period.

Criteria Group 8: Common Criteria Related to Change Management

CC 8.0 Common Criteria Related to Change Management			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1	**The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**		
8.1.1	Change management procedures are in place to govern the modification of critical company information resources and address security requirements.	Inspected the Change Management and Control Policy to determine that change management procedures were in place to govern the modification of critical company information resources and address security requirements.	No exceptions noted.
8.1.2	The software and infrastructure change management process requires that change requests are: - Authorized; - Formally documented; - Tested prior to migration to production; and - Reviewed and approved.	Inspected the change request tickets and approvals related to a sample of network, BCC, and PlanetPress changes to determine that the software and infrastructure change management process required that change requests were: - Authorized; - Formally documented; - Tested prior to migration to production; and - Reviewed and approved.	There were no instances of a network, BCC, or PlanetPress change during the period; therefore, the control did not operate during the period.
8.1.3	Changes to critical company information resources are required to be documented and tracked from initiation through deployment and validation.	Inspected the change request tickets and approvals related to a sample of network, BCC, and PlanetPress changes to determine that changes to critical company information resources were required to be documented and tracked from initiation through deployment and validation.	There were no instances of a network, BCC, or PlanetPress change during the period; therefore, the control did not operate during the period.

CC 8.0 Common Criteria Related to Change Management			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1	**The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**		
8.1.4	Annual PCI vulnerability scans are performed. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum.	Inspected the most recent PCI vulnerability scanning results to determine that PCI vulnerability scans were performed within the year.	No exceptions noted.
		Inspected the remediation plan and tracking documentation to determine that a remediation plan was developed, and changes were implemented to remediate critical and high vulnerabilities at a minimum.	
8.1.5	A documented patch management process is in place.	Inspected the Patch Management Policy to determine that a documented patch management process was in place.	No exceptions noted.
8.1.6	Domain server patches are configured to automatically download updates. These updates are installed by appropriate personnel on a monthly basis.	Inspected the patching configurations and monthly change request tickets to determine that domain server patches were configured to automatically download updates, and that these updates were installed by appropriate personnel on a monthly basis.	**Exceptions noted.**
Exceptions noted: Domain server patches and updates were not installed on a monthly basis during the reporting period.			
Management's response: We acknowledge that this was an oversight. Our server was initially configured for manual updates, meaning our provider had to physically come on-site and initiate the process. We have reconfigured the server for automatic updates. These updates, if available, are downloaded and installed daily at 3:00 a.m.			

Criteria Group 9: Common Criteria Related to Risk Mitigation

CC 9.0 Common Criteria Related to Risk Mitigation			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**		
9.1.1	A risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment Policy to determine that a risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
9.1.2	Cyber insurance is in place to minimize the financial impact of any loss events.	Inspected the cybersecurity insurance documentation to determine that cyber insurance was in place to minimize the financial impact of any loss events.	No exceptions noted.
9.1.3	An IT risk assessment is performed at least annually to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	Inspected the annual risk assessment documentation to determine that an IT risk assessment was performed within the year to identify the information security risks to the organization that would impact the achievement of service commitments and system requirements.	No exceptions noted.