SOC-2 Certification for Data and Privacy

MAIL LOUISVILLE, INC

Mail Louisville, Inc.

Independent Service Auditor's Report on Controls at a Service Organization Relevant to the Security Trust Services Criteria on the Mail Louisville Information Technology General Control Environment.

For the period October 1, 2020 to December 31, 2020

DHG

An Independent Service Auditor Report issued by
Dixon Hughes Goodman LLP

table of contents

section I: independent service auditor’s report 1

section II: management’s assertion 4

section III: management’s description of its system and controls 5

section IV: description of trust services criteria, related controls, and results 14

This report, including the description of tests of controls and results thereof, 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 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding. This report is not intended to be, and should not be, used by anyone other than these specified parties.

section I: independent service auditor's report

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

Scope

We have examined Mail Louisville, Incorporated'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, 2020 to December 31, 2020 (description) based on the criteria for a description of a service organization's system set forth in DC section 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, 2020 to December 31, 2020, 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 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 the following:

- 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.
- 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 of this report.

Opinion

In our opinion, in all material respects,

- the description presents Mail Louisville's information technology control environment (system) that was designed and implemented throughout the period October 1, 2020 to December 31, 2020 in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period October 1, 2020 to December 31, 2020 to provide reasonable assurance that Mail Louisville's service commitments and system requirements would be achieved based on the applicable trust services criteria, 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, 2020 to December 31, 2020 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 entities 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 control environment (system) during some or all of the period October 1, 2020 to December 31, 2020, business partners of Mail Louisville subject to risks arising from interactions with the Mail Louisville information technology 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, 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
- 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, South Carolina

February 18, 2021

section II: management's assertion

We have prepared the accompanying description of Mail Louisville's information technology control environment (system) titled "management's description of its system and controls" throughout the period October 1, 2020 to December 31, 2020 (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 Mail Louisville information technology 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)* were achieved.

The description indicates that 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 the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1) The description presents Mail Louisville's information technology control environment system that was designed and implemented throughout the period October 1, 2020 to December 31, 2020 in accordance with the description criteria.

2) The controls stated in the description were suitably designed throughout the period October 1, 2020 to December 31, 2020 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, 2020 to December 31, 2020 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") is based out of East Louisville, Kentucky that offers Custom Mail Lists, Graphics Design, Fulfillment, Four Color Variable Printing and Mailings of all types. Mail Louisville has been providing Direct Mail Fulfillment across the U.S. since 1995.

Fulfillment Services

Mail Louisville, Inc. provides handling and storage for clients who distribute promotional materials, brochures, or ship products. Orders can be sent via the Web, e-mail, hard copy, telephone, or fax. Mail Louisville will assemble kits, bundle brochures and ship material to client customers.

Statement Mailings

Mail Louisville, Inc. specializes in statement and invoicing solutions for our customers. This multiple step process includes a quality control system and leverages commercial off-the-shelf technology. Within this service offering, Mail Louisville assists customers with designing the form layout for postal optimization and document integrity.

Laser Printing

Mail Louisville's wide range of printing capabilities includes four color digital ink jet presses as well as an envelope press. Variable Data is utilized to be specific to customer's request.

Drop Ship to NDC/SCF

Drop Shipping is the process of transporting and depositing mail at a postal facility closer to the destination before transferring the mailings over to the Postal Service. Mailings are shipped to a Network Distribution Center (NDC) that serves a large geographical area or a Sectional Center Facility (SCF) that serves a smaller more defined geographical area.

Ink Jet Addressing

Mail Louisville provides Ink Jet addressing services utilizing equipment that transfers information from client databases directly onto the client's mail piece.

Postage Metering

Mail sent in large quantities can have postage applied with a postage meter rather than individual stamps. Metered mail is a more efficient way of handling postage for high-volume situations. The meter imprint allows customer mail to bypass several United States Postal Service (USPS) processing steps.

Folding & Inserting

Mail Louisville folding machines perform folding and inserting services from a single sheet to complex mailings which can include blind matching, collating, sorting, hand inserts, and sealing.

Tipping, Score and Glue

Mail Louisville provides tipping and scoring services using technology systems that score, tip a business card or magnet, then fold and glue client documents.

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.
- 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

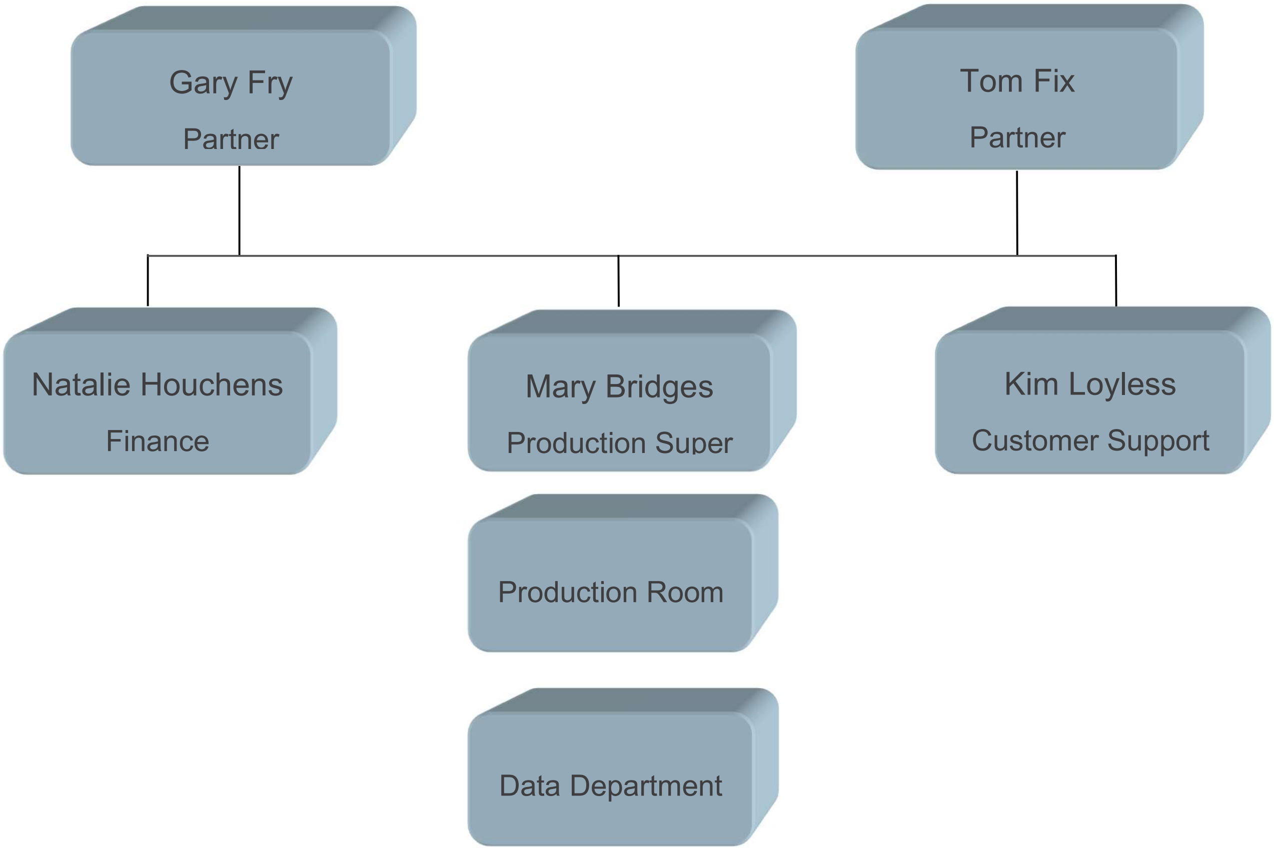
BCC Software, originally Business Computer Center, Inc., is a third party postal and presort software solution. Mail Louisville Data Specialists utilize BCC Software that resides in-house to cleanse and fix addresses provided by clients via incoming file types that include Excel, CSV, XML, TXT, Delimited, 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, Risk Assessment, Monitoring, and Information and Communication

Organizational 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
- Assignment of authority and responsibility

Integrity and Ethical Values

A Code of Business Conduct and Ethical Standards is reviewed, updated if applicable, and approved by senior management annually. Personnel are required to read and accept the Code of Business Conduct and Ethical Standards upon their hire and formally reaffirm them annually thereafter. The Company's Code of Business Conduct 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 and Risk Mitigation

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

1. Scope the assessment
2. Gather information
3. Identify threats

4. Identify vulnerabilities
5. Assess security controls
6. Evaluate the potential impact of findings
7. Determine the level of risk
8. Recommend security controls to mitigate identified risks
9. 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;
- 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.

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
User organizations are responsible for performing annual user access reviews to Mail Louisville's SFTP portal.	CC 6.0
User organizations are responsible for confirming access to the Mail Louisville services is immediately disabled for terminated user entity personnel.	CC 6.0
User organizations are responsible for changing passwords to Mail Louisville's SFTP portal periodically – at least every 90 days.	CC 6.0
User organizations are responsible for deleting their personal data from Mail Louisville resources when necessary.	CC 7.0
User organizations are responsible for notifying Mail Louisville of any issues, problems, or needed changes.	CC 8.0

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, 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.

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 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 Ethical Standards is reviewed, updated if applicable, and approved by senior management annually.	Inspected the Code of Business Conduct and Ethical Standards to determine whether it outlines the service organization's commitments to integrity and ethical values and if the conduct and standards were updated and approved by senior management within the examination period.	No exceptions noted.
1.1.2	Personnel are required to read and accept the Code of Business Conduct and Ethical Standards upon their hire and formally reaffirm them annually thereafter.	For a selection of new hires, inspected the Code of Business Conduct and Ethical Standards signed to determine whether the conduct and the standards were acknowledged by each new hire selected. For a selection of current personnel, inspected the signed Code of Business Conduct and Ethical Standards to determine whether the conduct and the standards were acknowledged by each person selected.	No exceptions noted.
1.1.3	The Company's Code of Business Conduct includes a sanctions policy for personnel who violate the Code of Business Conduct.	Inspected the Company's Code of Business Conduct to determine whether it included a sanctions policy for personnel who violate the Code of Business Conduct.	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 1.1	**The entity demonstrates a commitment to integrity and ethical values.**		
1.1.4	Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks.	For a selection of new hires, inspected the background checks to determine whether selected personnel successfully completed background checks including criminal (as needed), and drug checks prior to being hired by the Company.	No exceptions noted.
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 contractual agreements in place with the staffing agency in use to determine requirements for background checks are required to be completed prior to onboarding at Mail Louisville.	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 Company's organizational chart to determine whether organizational structure, reporting lines, authorities, and responsibilities were established and updated.	No exceptions noted.
1.3.2	Job descriptions are reviewed by management on an annual basis for needed changes.	Inspected evidence of job description reviews to determine whether job descriptions were reviewed by management on an annual basis and revised, if necessary.	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 organizational structure and a sample of job descriptions to determine whether organizational structure, reporting lines, authorities, and responsibilities were documented.	No exceptions noted.
1.3.4	The confidentiality commitments and obligations of user entities (clients) providing sensitive data to the company are included in standard services agreements.	For a selection of user entities (clients) providing sensitive data, inspected the signed services agreements to ensure confidentiality requirements were documented and client obligations were defined.	**Exceptions Noted.**
Exception Noted: A Master Services Agreement was not available for one (1) of three (3) sampled user entities providing sensitive data to Mail Louisville.			
Management's Response: Client selected has no Master Services agreement on file because the client does not provide sensitive data to Mail Louisville but does utilize the Mail Louisville SFTP for data transmissions. Client submits color copy documents for printing that have no personal or confidential data included. Mail Louisville will present a Master Services Agreement to the selected client.			
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.	For a selection of current employees, inspected the job descriptions to determine whether job requirements were documented including responsibilities and skills.	No exceptions noted.
1.4.2	Annual performance appraisals are performed with Mail Louisville personnel to evaluate performance in their roles with the Company.	For a selection of personnel, obtained the corresponding performance appraisals to determine performance is being continually evaluated.	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.	For a selection of new hires, inspected the background checks to determine whether selected personnel successfully completed background checks including criminal (as needed) and drug checks prior to being hired by the Company.	No exceptions noted.
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 Information Security Policies to determine if the policy defines responsibilities for maintaining and updating Information Security policy and procedures.	No exceptions noted.
1.5.2	Management has assigned responsibilities for implementation of the entity's Information Security policies to the senior management.	Inspected the corporate bylaws to determine whether senior management was charged with establishing, maintaining, and enforcing the overall security policies and procedures.	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 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 Company's annual risk assessment to determine whether it identifies the information required to support internal controls and the achievement of the Company's 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.	Inspected the Company's annual IT risk assessment to determine whether it identifies potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements.	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 Company's documented policies and procedures as they relate to security to determine whether internal controls for producing timely, current, accurate, complete, accessible, protected, verifiable and retained information have been documented.	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 Company's internal Network share drives to determine whether documented policies and procedures are available to internal personnel.	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 meeting minutes to determine that the Special Meeting Group discussions are documented and address key items with respect to the achievement of the Company's service commitments and system 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 Company's documented incident response policies and procedures to determine whether it includes escalation tree and communication plans depending on the nature of the incident, including escalation to senior management, as necessary.	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.	For a sample of newly hired employees, inspected the onboarding packets to ensure security commitments are communicated and acknowledgements are retained.	No exceptions noted.
2.2.5	Management has developed in-house trainings describing its security commitments and requirements for personnel to support the achievement of objectives.	Inspected documentation of the Company's training content to determine security commitments and personnel requirements as they relate to organizational objectives to ensure they are properly included.	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 drive to determine Mail Louisville personnel have access to current policies and procedures. Inquired of management to determine whether changes to commitments that occurred during the examination period were communicated to internal users.	No exceptions noted.
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 procedures are in place guiding personnel on the appropriate use of Mail Louisville assets.	No exceptions noted.
2.2.8	Policies and procedures are reviewed and updated no less than annually.	Inspected a sample of policies and procedures to determine whether a history of changes with the date of change was documented.	No exceptions noted.
CC 2.3	**The entity communicates with external parties regarding matters affecting the functioning of internal control.**		
2.3.1	Agreements are established with clients providing sensitive data that include clearly defined terms, conditions, and responsibilities for the company and clients.	For a selection of clients who provide sensitive data, inspected the agreements, and determined that the agreement outlined the Company's requirements, including terms, conditions, and responsibilities.	**Exception noted. See conclusion at CC 1.3.4**
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 Company's documented Incident Response policies and procedures to determine whether they include an escalation tree and communication plans depending on the nature and severity of the incident.	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.**		
2.3.3	Contact email addresses and phone numbers are made available on the Company's websites.	Inspected the Company's website to determine whether contact email addresses and phone numbers are available to customers and external users.	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 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 Company's annual risk assessment to determine whether it identifies the information required to support internal controls and the achievement of the Company's service commitments and system requirements.	No exceptions noted.
3.1.2	Updates or modifications to standard contractual terms and commitments are approved by management prior to contract approval.	Inspected a sample of Master Services Agreements to determine whether standardized contractual language is included and if any changes to that language are tracked and approved.	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 a sample of meeting minutes to determine whether quarterly meetings are held where organizational strategy and operations, and other critical factors to the business were discussed.	No exceptions noted.
3.2.2	An annual risk assessment is performed to identify risks arising from external and internal sources.	Inspected the annual risk assessment to determine whether risks arising from external and internal sources and effectiveness of controls to mitigate those risks were identified.	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 risk assessment.	Inspected a sample of minutes and meeting agendas from quarterly Special Meetings to determine whether security risks and vulnerabilities identified during the Company's annual risk assessment were assessed, and analyzed by management.	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 a documented classification scheme for labeling and handling data is in place.	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 purchasing authority designations and limits assigned to management within the Shareholders Agreement to determine only authorized employees can purchase 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	Special Meetings are held on a periodic basis to discuss strategy and operations, and other factors critical to the business.	Inspected a sample of meeting minutes to determine whether quarterly meetings are held where organizational strategy and operations, and other critical factors to the business were discussed.	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 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 Company's annual risk assessment to determine whether it identifies the information required to support internal controls and the achievement of the Company's 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 annual risk assessments and communicates results to management for monitoring of corrective actions.	Inspected documentation for the annual reviews of the risk assessment and any corrective action plans developed as a result of the assessment.	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 annual PCI vulnerability scan to determine whether vulnerability scans were performed, and remediation plans were developed to remediate critical and high vulnerabilities.	No exceptions noted.
CC 4.2	**The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**		
4.2.1	Management performs annual risk assessments and communicates results to management for monitoring of corrective actions.	Inspected documentation for the annual reviews of the risk assessment and any corrective action plans developed as a result of the assessment.	No exceptions noted.
4.2.2	Deficiencies are risk rated and reported to senior management, as needed.	Inquired of management to determine whether management meets periodically to discuss planned assessments, identified risks, and on-going remediation.	No exceptions noted.
		Inspected the meeting minutes from the annual Special Meeting to determine whether risks are reported to senior management.	

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 action, including senior management and the board of directors, as appropriate.**		
4.2.3	Management tracks the status of deficiencies until satisfactorily resolved.	Inspected the annual PCI vulnerability scan to determine whether vulnerability scans were performed, and remediation plans were developed to remediate critical and high vulnerabilities.	No exceptions noted.
		Inspected applicable meeting agendas to determine whether risks are reported to senior management.	

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 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 Company's annual risk assessment to determine whether it identifies the information required to support internal controls and the achievement of the Company's service commitments and system requirements.	No exceptions noted.
5.1.2	Senior management is responsible for the implementation, maintenance, and effectiveness of the information security program.	Inspected the Security Policy to determine whether senior management is charged with establishing, maintaining, and enforcing the overall security policies and procedures.	No exceptions noted.
5.1.3	The Company has designed application-enforced segregation of duties to define what privileges are assigned to users within applications.	Inspected the access control policy to determine whether application controls were designed to enforce segregation of duties to users within applications.	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	As part of IT strategic planning, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.	Inspected the meeting minutes of the annual Special Meeting to determine whether IT risk affecting the organization and recommended courses of action were identified and discussed.	No exceptions noted.
5.2.2	An 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 Company's annual risk assessment to determine whether it identifies the information required to support internal controls and the achievement of the Company's service commitments and system requirements.	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 5.3	**The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**		
5.3.1	The Company's policy and procedure manuals address controls over significant aspects of information security.	Inspected the policy and procedure manuals to determine whether they included section headings that addressed controls over the significant aspects of information security.	No exceptions noted.
5.3.2	Senior management is charged with establishing, maintaining, and enforcing the overall security policies and procedures.	Inspected the Security Policy to determine whether senior management is charged with establishing, maintaining, and enforcing the overall security policies and procedures.	No exceptions noted.
5.3.3	The Company's policy and procedure manuals are reviewed annually by senior management.	Inspected documentation of the annual review of the policy and procedures manuals by senior management.	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 whether a listing is in place to track system 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 login attempts to determine whether the in-scope system components require unique usernames and passwords for 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. Evidence of the annual review is maintained within meeting minutes with the Board of Directors.	Inspected the most recent annual access review documentation to determine whether an access review was performed for in-scope system components and if inappropriate access was removed, as necessary.	No exceptions noted.
6.1.4	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine if procedures exist around classifying and protecting confidential information.	No exceptions noted.
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.	Inspected the Network password configurations to determine whether passwords are configured according to Company 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 6.1	**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.**		
6.1.6	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.	Inspected in-scope system components to determine whether passwords are configured according to Company policy.	No exceptions noted.
6.1.7	The Change Control policy requires that system changes undergo formal documentation, review, and authorization.	Inspected the Change Control policy to determine whether changes to the system are to be documented, reviewed, and approved.	No exceptions noted.
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 access request forms for a sample of new hires that received access to the in-scope system components to determine whether an access provisioning request was approved prior to access being provisioned.	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.**		
6.2.2	A termination checklist is completed, and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine whether terminated employees retained access to the in-scope system and platforms after their separation.	Control did not operate during the reporting period.
		Inspected termination tickets for a sample of terminated employees during the review period to determine whether access was revoked within 24 hours as a 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. Evidence of the annual review is maintained within meeting minutes with the Board of Directors.	Inspected the most recent annual access review documentation to determine whether an access review was performed for in-scope system components and if inappropriate access was removed, as necessary.	No exceptions noted.
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. Evidence of the annual review is maintained within meeting minutes with the Board of Directors.	Inspected the most recent annual access review documentation to determine whether an access review was performed for in-scope system components and if inappropriate access was removed, as necessary.	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.**		
6.3.2	A termination checklist is completed, and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine whether terminated employees retained access to the in-scope system and platforms after their separation. Inspected termination tickets for a sample of terminated employees during the review period to determine whether access was revoked within 24 hours as a part of the termination process.	Control did not operate during the reporting period.
6.3.3	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.	Inspected list of administrator accounts for the in-scope systems to verify access is limited to authorized users. Inspected a listing of Active Directory administrators to ascertain privileged access is limited to authorized users.	No exceptions noted.
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 and require badge access. Visitors must call for assistance to be granted access.	Examined the doors to the facility and inquired of management to determine entry/exit points throughout the facility are controlled through badge readers and visitors must check in prior to accessing the facility.	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.**		
6.4.2	A termination checklist is completed, and physical access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active server room badge listing to determine whether terminated employees retained access to the server room after their separation.	Control did not operate during the reporting period.
		Inspected termination checklists for a sample of terminated employees during the review period to determine whether physical access was revoked within 24 hours as a part of the termination process.	
6.4.3	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.	Inspected a sample of visitor logs to determine visitors are required to register at the front desk prior to accessing the facility	No exceptions noted.
		Inquired of management to determine visitors are escorted by an employee when accessing the facility.	
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 physical access review completed by management to determine whether physical access to the data centers was reviewed on an annual basis 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.	Examined the doors to the facility and computer rooms to determine whether ID cards are required for entry.	No exceptions noted.
		Inspected the audit logging configurations for the badge access system and access logs for a sample of access points to determine whether access key card usage is 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 data retention and disposal procedures to determine whether procedures are in place.	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 certificates of destruction for a sample of digital information system media to be destroyed to determine whether measures are being applied to properly dispose of physical assets.	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 employed within the environment to determine whether the permit rules align with the specified networking protocols permitted for inbound network traffic.	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 SFTP settings to determine whether transmission of confidential and/or sensitive information over public networks is encrypted.	No exceptions noted.
6.6.3	Intrusion detection systems are used to provide continuous monitoring of the network and prevention of potential security breaches.	Inspected intrusion detection system configurations to determine whether continuous monitoring of the network and early prevention of potential security breaches are in place.	**Exception Noted.**
Exception Noted: An Intrusion Detection System was not implemented until after the reporting period.			
Management's Response: The Cisco IDS system was purchased and installed during the last week of 2021 with configuration screenshots to DHG. All internal procedures were followed on this acquisition included an approved Change Control Form.			
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 Secure file transfer protocols (SFTP) server is restricted to the data specialists' group.	Inspected the listing of data specialists with access to the SFTP server to confirm access is appropriate.	No exceptions noted.
6.7.2	Secure file transfer protocols (SFTP) are deployed for transmission of confidential and/or sensitive information over public networks.	Inspected SFTP configurations to determine whether SFTP was used for the 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 Acceptable Use Policy to determine whether removable media is required to be encrypted and sanitized prior to use.	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 Ethical standards.	Inspected the Code of Business Conduct and Ethical Standards to determine whether the policies prohibit installation of software by users, and installation is limited to system administrators.	**Exception Noted.**
Exception Noted: The Code of Business Conduct and Ethical Standards does not prohibit the installation of software by users.			
Management's Response: The Code of Business Conduct and Ethical Standards has been updated to reflect this change. This has also been communicated to all employees on the Shared Drive.			
6.8.2	Local administrator access on end user devices is restricted to appropriate personnel.	Inspected a sample of end user devices to determine local administrator access rights are restricted to only 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 and availability requirements.	Inspected the change management procedures to determine whether procedures were in place to govern the modification and maintenance of critical company information resources and addressed security and availability requirements.	No exceptions noted.
6.8.4	Anti-malware technology is deployed for environments. This software is used to scan assets prior to being placed into production.	Inspected screenshots of anti-malware software configurations to determine whether anti-virus is updated routinely, logged, and installed on production servers.	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 annual PCI vulnerability scan to determine whether baseline security configurations are evaluated for potential vulnerabilities.	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 annual PCI vulnerability scan to determine whether vulnerability scans were performed, and remediation plans were developed to remediate critical and high vulnerabilities.	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 websites.	Inspected the Company's website to determine whether contact email addresses and phone numbers are available to customers and external users.	No exceptions noted.
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 written incident management procedures to determine whether the procedures include a process for handling security incidents.	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.**		
7.2.3	When an incident is detected or reported, a defined incident management process is initiated, and corrective actions are implemented in accordance with defined policies and procedures.	Selected a sample of security incidents logged in the incident tracking system to determine whether the defined incident management process is initiated and followed to resolution.	No exceptions noted.
7.2.4	Intrusion detection systems are used to provide continuous monitoring of the network and prevention of potential security breaches.	Inspected intrusion detection system configurations to determine whether continuous monitoring of the network and early prevention of potential security breaches are in place.	**Exception noted. See conclusion at CC 6.6.3**
7.2.5	Incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether the defined incident management process is initiated and followed to resolution.	No exceptions noted.
7.2.6	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.	Inspected the Company's annual IT risk assessment to determine whether it identifies potential threats and vulnerabilities to the achievement of the Company's service commitments and system requirements.	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	Security incident response policies and procedures have been developed that are communicated to authorized users.	Inspected incident response policies and procedures to determine whether an incident response plan is documented and has been communicated to authorized users.	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 7.3	**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.**		
7.3.2	Incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether the defined incident management process is initiated and followed to resolution.	No exceptions noted.
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 documentation of root cause analysis for a sample of IT security incidents to determine whether a root cause analysis was performed to determine the classification and impact of the event.	No exceptions noted.
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	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response.	Inspected security policies to determine whether the Company has established defined roles and responsibilities to oversee implementation of the incident response plan.	No exceptions noted.
7.4.2	After an incident has been confirmed, a defined incident management process is initiated, and corrective actions are implemented in accordance with defined policies and procedures.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel and corrective action plans were documented.	No exceptions noted.
7.4.3	Real-time incremental and daily full backups are configured for the databases.	Inspected backup configurations to determine whether real-time incremental and daily full backups are configured for the databases.	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 7.4	**The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**		
7.4.4	Incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether the defined incident management process is initiated and followed to resolution.	No exceptions noted.
7.4.5	Annual PCI vulnerability scans are performed on a periodic basis. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum.	Inspected the annual PCI vulnerability scan to determine whether vulnerability scans were performed, and remediation plans were developed to remediate critical and high vulnerabilities.	No exceptions noted.
CC 7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
7.5.1	Incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether the defined incident management process is initiated and followed to resolution.	No exceptions noted.
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 documentation of root cause analysis for a sample of IT security incidents to determine whether a root cause analysis was performed to determine the classification and impact of the event.	No exceptions noted.

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 procedures to determine whether procedures were in place to govern the modification and maintenance of critical company information resources and addressed 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 • Reviewed and approved	Inspected a sample of change requests to determine whether changes were: • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved	Control did not operate during the reporting period.
8.1.3	Changes to critical company information resources are required to be documented and tracked from initiation through deployment and validation.	Inspected a sample of change requests to determine whether changes were: • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved	Control did not operate during the reporting 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 on a periodic basis. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum.	Inspected the annual PCI vulnerability scan to determine whether vulnerability scans were performed, and remediation plans were developed to remediate critical and high vulnerabilities.	No exceptions noted.
8.1.5	A documented patch management process is in place.	Inspected the patch management policy to determine whether there are documented policies and procedures.	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 patch management configurations on the Domain server to ensure monthly patches are being applied automatically.	No exceptions noted.

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 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.	Inspected the risk management policy to determine whether a program has been established around 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 applicable insurance documentation to determine whether cyber insurance is in place for potential loss events to minimize the financial impact.	No exceptions noted.