System and Organization Controls 3 (SOC) 3 Report

Management's Report of Its Assertions on Vervent's Servicing System Based On the Trust Services Criteria for Security

For the Period July 1, 2019 to May 31, 2020

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Vervent

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over Vervent's Servicing System Based on the Trust Services Criteria for Security" (Assertion) that Vervent's controls over the Servicing System (System) were effective throughout the period July 1, 2019 to May 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Vervent management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Servicing System and describing the boundaries of the System;
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the Servicing System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, 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 management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of Vervent's Servicing System relevant security policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Vervent's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve Vervent's Servicing System's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; b) breakdown of internal control at a vendor or business partner; and c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, management's assertion that the controls within Vervent's Servicing System were effective throughout the period July 1, 2019 to May 31, 2020 to provide reasonable assurance that Vervent's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

September 1, 2020
Orange, California

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER VERVENT'S SERVICING SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY

September 1, 2020

Scope

We, as management of Vervent, are responsible for:

- Identifying the Vervent Servicing System (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled Description of Vervent's Servicing System (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment A) Description of Vervent's Servicing System;
- Identifying, designing, implementing, operating, and monitoring effective controls over Vervent's Servicing System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

Vervent utilizes Sypnotek (sub-service organization) to provide technical support and hosting services for Vervent's private cloud environment. The Description (Attachment A) includes only the controls of Vervent. The Description also indicates that certain trust services criteria specified therein can be met only if sub-service organization's controls assumed in the design of Vervent's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the sub-service organization. However, we perform annual due diligence procedures for third-party sub-service organization and, based on the procedures performed, nothing has been identified that prevents the sub-service organization from achieving their specified service commitments.

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

We assert that the controls within the system were effective throughout the period July 1, 2019 to May 31, 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security set forth in the AICPA's TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice organizations and user entities applied the complementary controls assumed in the design of Vervent's Servicing System controls throughout the period July 1, 2019 to May 31, 2020.

Vervent

SECTION THREE:

ATTACHMENT A: DESCRIPTION OF VERVENT'S SERVICING SYSTEM

Overview of Vervent's Operations

Vervent is an industry leading servicing solutions company that headquartered in San Diego, CA, and has an industry-leading team of professionals with extensive knowledge and experience backed up by a state-of-the-art technology platform. To ensure our clients are fully supported, we custom built and operate three state-of-the-art operations centers located in Baja California, Mexico, Portland, OR, and at our HQ in San Diego, CA. Vervent Baja is our largest ops center with an 1,110 seat-capacity and is located just 30 minutes from our San Diego location across the San Diego/Tijuana border. This center provides us with a nearshore model that offers full operations oversight from our leadership team with the economic advantage of operating in Mexico. Vervent Portland includes a 200-seat center where we handle calls, non-voice operations and keep our IT command center. Vervent San Diego houses corporate and executive staff, along with a 100-seat operations center. Vervent's clients include financial institutions, private equity groups, and other consumer and commercial finance entities.

Vervent is also the leading provider of best in class servicing for both unsecured and titled asset portfolios. Our professionals are committed to providing the highest level of service to borrowers while maximizing lender and investor returns.

Vervent services wide spectrum of debt obligations, including:

- Unsecured Consumer
- Purchase Finance
- Student
- Autos
- Green & solar energy
- Powersports
- Elective medical procedures
- Small Business

Overview of the System and Applications

System Overview

New User Organizations

Data completion, accuracy, and security are a key step in setting up new user organization within Vervent' systems. Only the authorized personnel of the Operations staff have the

authorization to add new user organizations into the Nortridge Loan System (NLS). Once the organization is set up in Vervent's Servicing System (VSS), the accuracy and completeness of the new user organization setup is compared/verified to the user setup form by a second person and acknowledged. When errors are detected, they are remediated promptly.

Validation

Upon the completion of the loan or lease boarding, a report is reviewed to compare the data loaded against the raw boarding data. Additionally, a sample of new accounts (debtors) boarded into Vervent VSS is verified for accuracy and completeness by a second person. Upon review, if an error is found, the boarding data is compared to the Vervent VSS specifications to identify the source of the issue. If it is due to incorrect mapping, then the correct data is reloaded. If the error it is due to inaccuracy of the boarding data, then the client is consulted for further direction on remediating the issue.

Confirmation

Documented account boarding confirmation reports are sent to the user organizations per the servicing contract once the debtor information is uploaded into Vervent's VSS. Upon the client's review, if an error is found then the boarding data is compared to the data loaded into the system. If the incorrect field was loaded, then the correct information is reloaded, if it was due to inaccurate boarding data then additional information is requested from the client.

Assurance

For user organization changes, a semiannual audit is performed by someone other than the person who made the change in Vervent's VSS to ensure the change was authorized in writing from an appropriate person and the changes made in Vervent's VSS were verified to the source document.

For verbal debtor change requests for address and phone numbers received over the phone, a semiannual audit is performed by someone other than the person that made the debtor record change in Vervent's VSS to ensure the change was logged and commented in the Loan Field History Report.

For written debtor change requests, a semiannual audit is performed by someone other than the person that made the debtor record change Vervent's VSS to ensure the source documents matched the change logged in the Loan Field History Report.

Data Traffic

Data traffic movement is controlled and routed based on client profiles via Citrix Sharefile and Secure FTP. Clients only have the ability to view information maintained under their profiles. Vervent allows clients to view information with various access levels within their organization. Client information is segregated into sub-databases within the main database, and this configuration prevents data comingling.

Servicing

Vervent adheres to their documented servicing agreements; these agreements vary by user organization. Authorized personnel review account files and logs to verify accounts are properly serviced. These personnel receive alerts regarding the status of the shorts and delinquencies. Corrective action is taken as appropriate when issues are identified by alerting staff of operational or procedural changes via email or interoffice job aids.

Loan Advisory

Vervent creates and customizes loan advisory activity procedures and strategy in consultation with user organization. VSS will be utilized in performing loan advisory activity.

A monthly audit is performed for servicing delinquent accounts to verify timely distribution of late notices and frequency of collection calls, and follow-up campaigns (e.g. voice alerts, text messages, and letters). If inconsistencies or ineffective methods are found in the delinquent activities performed, then the strategies are reviewed and modified as needed. Debt settlements are processed in accordance with pre-established approval levels established by clients of Vervent. If a borrower is requesting a settlement outside of the established parameters, then Vervent determines if the request appears to be reasonable, and if so, then reasonable requests are forwarded to the client for review and authorization. A Form 1099-C is prepared and issued automatically for all applicable debtor accounts in which all or a portion of the debt was forgiven/settled.

Payment Processing

Vervent posts and deposits all payments or like monies received on the user organization's accounts within the number of day(s) of receipt as specified in the user organization contract. Receipts are applied to the debtor accounts in the order identified in the VSS. Vervent's bank provides lockbox services for payments received and controls when the debtors' remittances are processed. Vervent's reporting determines and ensures that the payments are processed as of the appropriate effective date (date of receipt).

Reconciliation

The accounting system general ledger, bank account, and VSS postings are reconciled for accuracy on a daily basis by Accounting Department and reviewed by a second level of management.

Segregation

The monies collected for the debtor accounts are segregated from the Vervent operating account.

Back-Up

Vervent monitors the replication of data daily via scripts and query to ensure the replicated database is up to date. In addition, the remote backup copies are periodically restored to another copy of the database and accessed to ensure the data is consistent with production.

Destruction Retention

A Destruction Retention Policy and Schedule has been established and communicated to all employees to maintain historical user organization transaction data.

Reporting

Vervent's authorized personnel reconcile report data for completeness and review for accuracy prior to distribution to the user organization. Reports to the user organizations vary, but may consist of Cash, Trial Balance, Aging, Paid Off Loans, and New Loan Boarding reports. Reconciliation includes (but is not limited to) the cash posted VSS being compared to the accounting application, reconciliation of the change in principal balances, and other deductions and servicing fees. This allows management to identify any discrepancies that may arise, which may require further review to determine source or cause of the difference and appropriately account for it prior to releasing and remitting the funds to the user organizations.

Each user organization has an internally prepared checklist based on the reporting requirements in the servicing agreement that is completed by the Investor Reporting Department and signed off by a secondary reviewer as verification of accuracy and completeness.

Distribution

Portfolio reports are distributed to the user organization in a timeframe specified by the user organization contract. Not all user organizations receive all the same standard reports, as some may not be applicable to the user organization's portfolio. However, report packages may typically include Cash, Aging, Trial Balance, New Loan Report, Paid-off Report, Capitalized Interest, and Write-Off Report.

Billing

Monthly service fees for current, delinquent, and defaulted accounts are calculated based on the terms of the Servicing and Billing Agreement for each user organization. Prior to release of the report to the user organization, the amounts due to Vervent and billed via an invoice or as a deduction from the remittance due to the user organization, is reviewed by a secondary reviewer. If any discrepancies are identified, they are then corrected prior to finalizing.

For remittances other than monthly, all debtor monies received by Vervent are remitted back to the user organization per servicing contract but only after a secondary review of the reconciliation is completed successfully. Should any discrepancies arise during the review, corrections are then affected (if applicable) before the funds are released and remitted to the client.

Remittance

For monthly remittances, all debtor monies received by Vervent less the servicing fees (when applicable) are remitted back to the user organization on a specific day as set forth in the servicing contract.

The calculation of the gross monies collected less the monthly service fees (if applicable) to Vervent, statements of other deductions, and the remittance amounts are reconciled by the Investor Reporting Department and reviewed prior to being distributed to the user organization. If discrepancies are detected during the review, the report is corrected (as applicable) prior to sending it to the user organization or remitting funds to either the user organization or Vervent.

General Technology Policy

Vervent has a General Technology Policy and Procedure, which includes passwords, handling of private information, network usage, Internet usage, and email usage. The policy is developed by the CTO and reviewed and approved by executive management. New hires sign an acknowledgement receipt of the policy which is retained by HR.

The Operations Department has the logical security permissions to set up or modify user organization information in the VSS. An annual audit is performed by senior management and reviews a sample of changes for accuracy. Similarly, for debtor loan level changes (such as loan amount, interest rate, payment amount, maturity date, etc.), only the Operations Department has access to make these changes. Additionally, changes to the debtor taxpayer identification number field and debtor contact information is restricted to the Delinquency group and Operations Department.

Windows, VSS, the accounting system, Citrix Sharefile, SFTP, are assigned unique user IDs and permissions for new hires and job modifications with prior authorization.

Windows, VSS, the accounting system, , Citrix Sharefile, SFTP permissions are disabled within 24 working hours for terminated employees. Windows remote access administrator access is granted with prior authorization.

Password policies exist, are monitored, and configured through Active Directory, and are enabled for Windows, VSS and the accounting system for a minimum password length, change frequency, password history, and password complexity.

Security logs are sent to a central SIEM and reviewed weekly by Vervent Information Technology and Information Security personnel for any potential security violations or attempts at unauthorized access.

Windows remote access requires management and COO approval and uses a two-factor authentication system. Remote access attempts and results are logged and reviewed monthly.

Handbook, Confidentiality, and PII disclosure

All new employees receive an employee handbook upon being hired and must sign an Acknowledgment of Receipt of Employee Handbook. The Employee Handbook is updated at least annually to include significant changes to state or federal laws or to the industry environment. When necessary, amendments may be made to the Employee Handbook outside of the update cycle.

All employees and subcontractors must sign a "Confidentiality and Non-Disclosure Agreement" upon being hired. Vervent maintains documented policies and procedures which define personally identifiable information (PII) and the appropriate use of the data.

Training

Training is required for the loan advisory new hires on collection laws, loan levels and collection procedures. Annual internal recertification for existing collection staff and customer service occurs for the Fair Debt Collection Practices Act (FDCPA), Fair and Accurate Credit Transactions Act (FACTA) and the Fair Credit Reporting Act (FCRA).

Background Checks

Background checks are performed on employees before they are given physical or logical access to facilities or systems. Only employees who have been appropriately vetted are offered employment.

Evaluations

Performance evaluations of existing collection staff are performed annually in January for the previous calendar year.

Security

Access into the Vervent office suite requires issuance of an electronic badge or enrollment to Vervent's biometric security system upon hire. Once access to Vervent's suite is received, based on the employee's work hours, HR activates the user's security access for use. Physical keys to the secure rooms requires authorized issuance based on employee status approved by the COO.

Badge access and/or possession of a room key, if issued, is revoked within 24 working hours for terminated employees by the HR department who controls all badge access to the office premises.

Visitors are required to sign a visitor log at the reception desk upon entering the office and are escorted at all times by a Vervent employee.

Scope

The scope of the review includes Vervent's servicing system for titled assets and unsecured loan and lease portfolios.

Control Environment

Key facets of the Company's control environment relating to processing and staffing for all processes performed by the Company are summarized below. These areas include:

- Integrity and Ethical Values
- Commitment to Competence
- Management's Philosophy and Operating Style
- Human Resources Policies and Practices
- Organizational Structure and Assignment of Authority and Responsibility

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Vervent control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of Vervent ethical and behavioral standards, how they are communicated, and how they are reinforced in practices.

Commitment to Competence

Vervent management defines competence as the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Vervent has focused on hiring experienced employees for the various positions required for the business.

Management's Philosophy and Operating Style

Vervent management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. Management meetings are held regularly to discuss operational issues.

Human Resources Policies and Practices

Vervent Human Resources policies and procedures relate to employee hiring, orientation, training, evaluating, promoting, compensating, and remedial actions. The policies and standard operating procedures contain formal and documented policies that define responsibilities, standards, and expectations from its employees.

Organizational Structure and Assignment of Authority and Responsibility

Vervent organizational structure provides the framework within which its activities for achieving entity- wide objectives are planned, executed, controlled, and monitored. Vervent management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Vervent has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Risk Assessment

The Vervent team is committed to providing superior service to its clients across all facets of the organization and solution it delivers. Vervent has put into place various methods for identifying and managing risks that could affect Vervent's ability to provide secure and reliable online document management and organization services to its clients. The organizational structure of Vervent ensures the segregation of duties across critical roles which service its clients. Access to sensitive client information is kept to the minimum access necessary to perform job functions and is permitted for authorized individuals only. Vervent proactively reviews on an annual basis key internal business processes which service clients in order to mitigate risks to gaps in delivery of its services to its clients and streamline operations.

Monitoring

The CTO monitors the quality of internal control performance as a normal part of his activities. The CTO is heavily involved in day-to-day activities and regularly reviews various aspects of internal and customer-facing operations to (i) determine if objectives are achieved, (ii) identify any new risks that develop, and (iii) implement appropriate measures to address those risks. Vervent, adopts a proactive approach to the monitoring of application security to ensure that any issues or risks are addressed before becoming significant problems.

Monitoring of the Subservice Organization

Vervent utilizes a Managed Service Provider, Synoptek, to provide technical support and hosting services for Vervent's private cloud environment. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at Synoptek, alone or in combination with controls at Vervent, to provide assurance that the required trust service criteria in this report are met.

Synoptek	
Criteria	**Control**
6.1.8	Key management is in place to support cryptographic techniques established by the Company.
6.8.3	Anti-virus software is installed on all servers and workstations. Updates are pushed to the nodes as new updates and signatures become available
8.1.6	Vendor security patches are evaluated, and critical patches are applied to key systems and applications within 30 days of release.
Vervent Management receives and reviews the Synoptek SOC report on an annual basis, including the Complementary User Entity Controls (CUECs) included within the report. In addition, through its daily operational activities, management monitors the services performed by Synoptek to ensure that operations and controls expected to be implemented are functioning effectively.	

Information and Communication

Description of Computerized Information Systems

Vervent utilizes industry-standard technologies to deliver secure, high performance information systems to clients, customers, and employees. State-of-the-art software as a service (SaaS) application provide the critical functions for servicing portfolios. Web portals and interactive voice response (IVR) enable borrower self-service for highly available and responsive customer self-service.

Servers are virtualized with VM vSphere housed in the collocation facility. Point to point fiber connectivity is utilized between the office and the collocation data center. A separate fiber Ethernet connection and a backup cable-based Ethernet (from a different service provider) circuit provide Internet connectivity and access to the cloud-based applications. Either Internet connection can be utilized for access to the collocation.

Collocation servers include the primary and backup domain controllers, SQL*Server for reporting and borrower portal, intranet file server, SFTP server. Vervent's primary Internet server is hosted in the same facility. Servers run Windows 2012R2 or later. Industry-leading backup and replication software is utilized to provide fast backup and recovery for virtualized servers.

Vervent utilizes its network to store all internal documentation related to sales, delivery, customer support, and administration which support its business and services to clients. Access to internal Vervent documentation is restricted based on functional area and job responsibilities. Vervent policies and procedures are also available through Vervent' internal network.

Communication

Management encourages open communication at all levels. The management team regularly distributes announcements regarding client project status highlights, company happenings, system changes, procedural changes, and other important information. Non-confidential information is openly shared across Vervent to encourage new ideas and continuous process improvement. Management has an "open door" policy and supports a cross-functional team approach to identify enhanced service offerings and support to its clients.

Description of Complementary User Entity Controls

The Vervent system was designed with the assumption that internal controls would be placed in operation by user entities. The application of such internal controls by user entities is necessary to achieve certain criteria identified in this report. There may be additional criteria and related controls that would be appropriate for the processing of user entity transactions which are not identified in this report.

This section describes certain controls that user entities should consider for achievement of criteria identified in this report. The complementary user entity controls presented below should not be regarded as a comprehensive list of all the controls that should be employed by user entities.

Data Validation

- Users are responsible for the accuracy of data into the system.

Provisioning Accounts

- Users are responsible for restricting authority of provisioning new user accounts within any Vervent website.

Termination Procedures

- Users are responsible for contacting Vervent in a timely manner to ensure terminated employee account access is removed.

Network Security

- Users are responsible for ensuring user owned or managed applications, platforms, databases, and network devices that may process or store data derived from Vervent are logically secured.

General Controls

- Users are responsible for ensuring user access to reports and other information generated from Vervent is restricted based on business need.
- Users of Vervent' hosted applications are responsible for maintaining appropriate IT General Computer Controls and Application Controls.

Regulatory, Compliance, and Service Agreements

- Users are responsible for adhering to all regulatory compliance issues when they are associated with Vervent in a service agreement.
- Users are responsible for reviewing and approving the terms and conditions stated in service agreements with Vervent.

SECTION FOUR:

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Vervent is an industry leading servicing solutions company headquartered in San Diego, CA. Led by an experienced team of professionals with extensive knowledge and industry know-how, their model focuses on accelerated service and is backed up by a cutting-edge technology platform. To ensure clients are fully supported, they custom built and operate three state-of-the-art operations centers located in Baja California, Mexico, Portland, OR, and at our HQ in San Diego, CA. Vervent Baja is their largest operations center with an 1,110 seat-capacity and is located just 30 minutes from the San Diego headquarters across the San Diego/Tijuana border. This center provides a nearshore model that offers full operations oversight from our leadership team with the economic advantage of operating in Mexico. Vervent Portland includes a 200-seat center where we handle calls, non-voice operations and keep our IT command center. Vervent San Diego houses corporate and executive staff and our compliance/legal team, along with a 100-seat operations center. Vervent's clients include financial institutions, private equity groups, and other consumer and commercial finance entities.

Vervent designs its processes and procedures related to Vervent's Management Systems (VMS) to meet all objectives for Vervent's services. Those objectives are based on the service commitment that Vervent makes to their clients.

Vervent's security commitments to user entities are documented and communicated in Client Agreements, as well as in the description of service offerings provided. The Vervent base security commitments include, but are not limited to the following:

- Security principles within the fundamental design of Vervent's Management Services that are designed to permit system users to access the information for their entity while restricting them from accessing information of other entities.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of firewalls and network segmentation restricting traffic flow to appropriate traffic.
- Logical access controls and regular review and monitoring of user access.
- Security monitoring infrastructure including intrusion detection, intrusion prevention, centralized log management, alerting through Vervent's Cybersecurity practice.
- Geographically separated data centers and cloud service providers with multi-layered physical security.
- Vulnerability Management program designed to identify and correct vulnerabilities within the environment in a timely manner.
- Incident Response program designed to minimize the impact and protection of resources.

- Continuous Cybersecurity awareness program including training and periodic testing of all Vervent employees.

Vervent establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Vervent's system policies and procedures, system design documentation, and client contracts. Information Security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the systems are operated, how the internal business systems and networks are managed, and how employees are hired and trained.