



System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on Vervent's Servicing System for title assets and unsecured loan, lease, and credit card portfolios Based On the Trust Services Criteria for Security

For the Period October 1, 2020 to September 30, 2021





TABLE OF CONTENTS

Section 1	Report of Independent Accountants	1
Section 2	Management’s Report of Its Assertions on the Effectiveness of Its Controls over Vervent’s Servicing System for title assets and unsecured loan, lease, and credit card portfolios Based on the Trust Services Criteria for Security	4
Section 3	Attachment A: Vervent’s Description of the Servicing System for title assets and unsecured loan, lease, and credit card portfolios	6
	Attachment B: Principal Service Commitments and System Requirements	10



SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of 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 for title assets and unsecured loan, lease, and credit card portfolios Based on the Trust Services Criteria for Security” (Assertion) that Vervent’s controls over the Servicing System for title assets and unsecured loan, lease, and credit card portfolios (System) were effective throughout the period October 1, 2020 to September 30, 2021, 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*).

The Assertion also indicates that Vervent’s (“Service Organization”) controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Vervent’s infrastructure’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Vervent uses a subservice organization to provide technical support and hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Vervent to achieve Vervent’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitable design or operating effectiveness of such complementary subservice organization controls.

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 for title assets and unsecured loan, lease, and credit card portfolios 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 for title assets and unsecured loan, lease, and credit card portfolios (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 for title assets and unsecured loan, lease, and credit card portfolios 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 for title assets and unsecured loan, lease, and credit card portfolios' 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.

Opinion

In our opinion, management's assertion that the controls within Vervent's Servicing System for title assets and unsecured loan, lease, and credit card portfolios were effective throughout the period October 1, 2020 to September 30, 2021 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

November 22, 2021
Las Vegas, Nevada



SECTION TWO: MANAGEMENT’S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER VERVENT’S SERVICING SYSTEM FOR TITLE ASSETS AND UNSECURED LOAN, LEASE, AND CREDIT CARD PORTFOLIOS BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY

November 22, 2021

Scope

We, as management of Vervent, are responsible for:

- Identifying the Vervent Servicing System for title assets and unsecured loan, lease, and credit card portfolios (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled Vervent’s Description of the Servicing System for title assets and unsecured loan, lease, and credit card portfolios (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 B)
- Identifying, designing, implementing, operating, and monitoring effective controls over Vervent’s Servicing System for title assets and unsecured loan, lease, and credit card portfolios (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.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period October 1, 2020 to September 30, 2021.

Vervent uses a subservice organization to provide technical support and hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Vervent, to achieve Vervent’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We assert that the controls within the system were effective throughout the period October 1, 2020 to September 30, 2021, 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 for title assets and unsecured loan, lease, and credit card portfolios controls throughout the period October 1, 2020 to September 30, 2021.

Vervent

ATTACHMENT A: VERVENT'S DESCRIPTION OF THE SERVICING SYSTEM FOR TITLE ASSETS AND UNSECURED LOAN, LEASE, AND CREDIT CARD PORTFOLIOS

System Overview

The System is comprised of the following components:

- **Infrastructure** - The physical and hardware components of a system (facilities, equipment, and networks)
- **Software** - The programs and operating software of a system (systems, applications, and utilities)
- **Data** - The information used and supported by a system (transaction streams, files, databases, and tables)
- **People** - The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- **Procedures** - The automated and manual procedures involved in the operation of a system

Infrastructure

The operations and corporate facilities are located in San Diego, CA. Vervent utilizes a combination local area network ("LAN") / wide area network ("WAN") to share data among its employees. The IT data centers are located in the Portland, OR and Sioux Falls, SD facilities and are accessible 24 hours a day, 7 days a week, and 365 days a year to authorized Vervent personnel. Vervent uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operations.

The Vervent Management Servicing Platforms are hosted both on-premises, and via private cloud service provider (CSP) environments across multiple availability zones for redundancy and disaster recovery purposes. Vervent does not own or maintain any hardware in the CSP data centers. Services operate within a shared security responsibility model, where the CSP is responsible for the security of the underlying cloud infrastructure, and Vervent is responsible for securing the Vervent Platform deployed in the CSP (e.g., IAM, Azure policies, operating system and application security, security group configuration, network traffic monitoring).

Vervent maintains three separate virtualized environments: production, staging, and development. Each environment is secured and accessible only by appropriate and authorized Vervent personnel.

Access to CSP production instances is allowed only through an encrypted channel from Vervent's enterprise network to ensure the privacy and integrity of data transmitted over the public network. VPN, SSH and/or SSL connections are secured using AES-256 bit or greater encryption. Administrative access is restricted to authorized administrators, who must

authenticate via a bastion host through a secure SSH key, IAM roles, and multi-factor authentication.

Software

The Vervent Management System platforms run in a virtualized environment with either Microsoft or Linux operating systems as the base. Monthly, the continuous integration platform runs an automated process to update the server and workstation images. A configuration management tool is used to configure software applications on individual instances using approved scripts.

Data

Systems integration to the Vervent Management Systems are configured with third parties via secure APIs. Vervent validates, processes, and stores data within the Vervent Management System platform. Data is stored on database servers running modern and supported versions of Microsoft SQL Server. All data is encrypted both at rest and in transit with a minimum of AES-256 bit encryption.

Data is provided to customers via various secure methods:

- Customers can access data, documents and reports via Vervent's secure online customer web portals.
- Reports can be configured to send to customers via one of several secure, cloud-based content sharing and/or managed file transfer platforms, on a defined schedule.
- Secure API integrations receive/transmit data to third-party platforms and services.

Under a managed services agreement, Vervent manages the product and data on behalf of the customer. As part of these services, Vervent typically provides reports of activity and status to the customer.

People

The following functional roles/teams comprise the framework to support effective controls over governance, management, security, and operation:

- *Board of Directors* establishes business and strategic objectives to meet the interests of stakeholders and provides independent oversight of financial and operational performance. A board of directors meets with the executive management team on a semi-annual basis, or more frequently as needed. Management presents operational and third-party assessment results to the board of directors upon completion. Board attendance is tracked, and discussion points and decisions are documented in board minutes. The board operates under bylaws that define responsibilities, including the oversight of management's system of internal control. The board consists of sufficient members who are independent from management and are objective in making decisions.

- *Executive Management* oversees, and is ultimately responsible for, all aspects of service delivery and security commitments. Among other responsibilities, Executive Management ensures that controls are enforced, risk assessment/management activities are approved and prioritized, people are appropriately trained, and systems and processes are in place to meet security and service requirements.
- *Compliance* is responsible for creating and maintaining a comprehensive Compliance Program to effectively handle all matters related to regulatory compliance, data privacy compliance, as well as ensure compliance with all applicable laws surrounding the services that Vervent provides. Compliance is also responsible for ensuring Vervent employees are aware of and actively complying with anything related to the aforementioned through the implementation of mandatory Compliance trainings.
- *Human Resources* is responsible for managing all functions related to recruiting and hiring, employee relations, performance management, training, and resource management. Human Resources partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with Vervent Company's mission, vision, and values.
- *Information Technology (IT)* management has overall responsibility and accountability for the enterprise computing environment. IT Operations personnel administer systems and perform services supporting key business processes, including architecting and maintaining secure and adequate infrastructure, monitoring network traffic, and deploying approved changes to production. The Application Development team is responsible for application development, initial testing of changes, and troubleshooting/resolving application issues.
- *Information Security* is responsible for identifying, assessing and managing risk, defining control objectives, monitoring performance of security controls, addressing and responding to security incidents, maintaining and communicating updates to security policies, and conducting security awareness training of all users.
- *Customer Success Managers (CSM)* are responsible for initiating the creation of new customer instances on the Vervent' Management System platform, adding users to new customer instances, providing user documentation to and coordinating training for new customers, and overall management of the account to ensure continued customer satisfaction.
- *Customer Support* is responsible for creating new customer instances on the Vervent Management System platform, fielding customer calls regarding the Vervent Management System platform services, initiating and responding to support tickets based on customer requests, and communicating with customers regarding any issues or outages.

Vervent is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. Vervent endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

Vervent has a Vice President of Information Security who is responsible for the design and oversight of security and privacy initiatives. The VP of Information Security reports directly to the CTO and indirectly to the Chief Executive Officer (CEO). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of the Vervent Management System platform. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CTO and VP of Information Security.

All employees are expected to adhere to Vervent’s IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

Incident Disclosure

No security incidents were detected or reported during the audit period.

Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of Vervent’s controls are suitably designed and operating effectively at the subservice organizations, along with related controls at Vervent.

Description of Complementary User Entity Controls

Vervent controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). Certain requirements can be met only if complementary user entity controls assumed in the design of Vervent’s controls are suitably designed and operating effectively, along with related controls at Vervent.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Company Background

Vervent sets the global standard for outperformance by delivering superior expertise, future-built technology, and meaningful services. We support industry-leading clients with primary strategic services including Loan & Lease Servicing, Credit Card Servicing/Full-Service Credit Card Programs, Backup Servicing/Capital Markets Support, Call Center Services, and Card Marketing & Customer Acquisition.

Vervent empowers companies to accelerate business, drive compliance, and maximize service. We are committed to providing the highest level of service to Vervent clients and their customers while maximizing lender and investor returns.

To ensure geo-redundant operations and fully support Vervent's clients, we custom built and operate five state-of-the-art operations centers located in Baja California, Mexico; Portland, OR; Sioux Falls, SD; Longview, TX; and HQ in San Diego, CA. Vervent Baja is the largest operations and communications center with a 1,110 seat-capacity facility and is located just 10 minutes across the border from San Diego. This center provides us with a nearshore model that offers full operations oversight from the Vervent leadership team with the economic advantage of operating in Mexico. Vervent Portland represents a 200-seat facility focused on non-voice operations and IT command center. Vervent Sioux Falls represents our Midwest operations center offering both voice and non-voice services and acts as the primary Credit Risk Management Hub. Vervent Longview is the largest of Vervent's US-based voice operations center with a 200+ seat agent capacity. Vervent San Diego houses corporate and executive staff, along with a 100-seat voice operations and service center. Vervent's clients include financial institutions, private equity groups, and other consumer and commercial finance entities. Vervent also works hand-in-hand with a wide variety of originator partners to ensure best-in-class service operations to help them manage their customer and collections needs.

Vervent services a wide spectrum of debt obligations, including:

- Credit Card
- Unsecured Consumer
- Purchase Finance/Marketplace Lending
- Student
- Auto & Powersports
- Green & Solar Energy
- Home Improvement
- Elective Medical Procedures
- Small Business

Description of Services Provided

Vervent's state of the art technologies and platform support management functions for title assets, unsecured loan, lease and credit card servicing:

- Vervent provides loan, lease and credit card servicing for a variety of clients, account products and asset classes including: installment loans, leases, call center services, credit cards, card marketing and customer acquisition and application processing.

The Vervent Platform consists of the following components:

- **Loan Management System:** Vervent Management System provides full spectrum loan servicing functionality for Vervent's clients.
- **Lease Management System:** Vervent Management System supports cradle-to-grave lease servicing capability including: lease management, collateral securitization, titling, UCC, insurance, and tax management.
- **Credit Card Management:** Vervent Management System integrates seamlessly with the industry's premier third-party card servicing platforms to provide highly customized, full lifecycle credit card programs including: card marketing and acquisition, application processing/underwriting, scoring, fulfillment and ongoing card management.

Principal Service Commitments and System Requirements

Vervent's security commitments to users entities are documented and communicated in client Master Services Agreements, as well as in the description of service offerings provided. The principal security commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of Vervent's Management Services platform and the customer data in accordance with Vervent's security requirements.
- Perform annual third-party security and compliance audits of the environment, including, but not limited to:
 - Reporting on Controls for a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 1 and SOC 2) examinations.
 - Payment Card Industry (PCI) Data Security Standard (DSS) Assessment
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of Vervent personnel with access to any systems.
- Prevent malware from being introduced to systems and workstations.

- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

Vervent establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and compliance regulations, and other system requirements. These requirements are communicated in Vervent's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards.

Vervent regularly reviews the performance metrics to ensure these commitments are met. If material changes occur that reduce the level of performance metrics within the agreement, Vervent will notify the customer via the prescribed communication methods.