System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on Vervent's Servicing Solution Based on the Trust Services Criteria for security

For the Period October 1, 2023 to September 30, 2024

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Vervent

Scope

We have examined Vervent ("Vervent") accompanying assertion titled "Assertion of Vervent Management" (assertion) that the controls within Vervent's Servicing Solution (system) were effective throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that Vervent'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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.*

Vervent uses subservice organizations to supplement its services. The description of the boundaries of the system presented in Attachment A 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 presents the types of complementary subservice organization controls assumed in the design of Vervent's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description of the boundaries of the system presented in Attachment A indicates that certain complementary user entity 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 presents the complementary user entity controls assumed in the design of Vervent'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

Vervent 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 Vervent's service commitments and system requirements were achieved. Vervent has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Vervent is responsible for selecting, and identifying in its

assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities
Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Vervent's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Vervent's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations
There are inherent limitations in the effectiveness of 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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion
In our opinion, management's assertion that the controls within Vervent's Servicing Solution were effective throughout the period October 1, 2023, to September 30, 2024, 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.

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

CyberGuard Compliance, LLP
February 14, 2025
Las Vegas, Nevada

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

February 14, 2025

Scope

We are responsible for designing, implementing, operating, and maintaining effective controls within Vervent's (Vervent) Servicing Solution (system) throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that Vervent'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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.* Our description of the boundaries of the system is presented in Attachment A (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Vervent's service commitments and system requirements were achieved based on the applicable trust services criteria. Vervent's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

Vervent uses subservice organizations to supplement its 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 organizations.

The description of the boundaries of the system also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Vervent's controls to achieve the service commitments and system requirements. The description presents the complementary user entity controls assumed in the design of Vervent's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Vervent's service commitments and system requirements were achieved based on the applicable trust services criteria.

Vervent

ATTACHMENT A: VERVENT'S DESCRIPTION OF THE BOUNDARIES OF ITS SERVICING SOLUTION

Company Background

Vervent sets the global standard for outperformance by delivering superior expertise, future-built technology, and meaningful services. Vervent supports its 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. Vervent is committed to providing the highest level of service to clients and their customers while maximizing lender and investor returns.

Vervent maintains geo-redundant operations and fully supports Vervent's clients, through six state-of-the-art operations centers located in Baja California, Mexico; Portland, OR; Sioux Falls, SD; Dumaguete, Philippines; Bangalore, India and at the headquarters in San Diego, CA. Vervent Baja is the second largest operations center with a 1,100 seat capacity and is located just 30 minutes from the San Diego location across the San Diego/Tijuana border. This center provides Vervent with a nearshore model that offers full operations oversight from Vervent's leadership team with the economic advantage of operating in Mexico. Vervent Portland represents a 150-seat capacity operations center predominantly focused on non-voice, finance and IT functions, as well as one of two IT command centers. Vervent Sioux Falls is the hub of the Credit Card and Risk Management departments and contains the second IT data center. Vervent Philippines is the largest operations center with a 1,300-seat capacity, providing BPO, operations and contact center functions. Vervent India was constructed as the Global Capability Center, with a 200+ seat capacity. Vervent San Diego houses corporate and executive staff, along with a 150-seat capacity operations center. Vervent's clients include financial institutions, private equity groups, and other consumer and commercial finance entities.

Vervent services a wide spectrum of debt obligations, including:

- Credit Card
- Unsecured Consumer Loans
- Purchase Finance/Marketplace Lending Loans and Leases
- Student Loans
- Auto & Powersports Loans and Leases
- Green & Solar Energy Loans and Leases
- Home Improvement Loans and Leases
- Small Business Loans and Leases
- Income Share Agreements Consumer and Commercial

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 operation.

The Vervent Servicing Solution platforms are hosted on-premises and via SaaS providers.

Logical controls separate the containerized production, staging, and development environments. 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 Servicing Solution platforms run in a containerized environment with Microsoft Operating System or Linux Operating System as the base. Monthly, the continuous integration platform runs an automated process to update the image. A configuration management tool is used to configure software applications on individual instances using approved scripts.

Data

Inbound integrations to the Vervent Servicing Solution are configured with third parties via Vervent utilizing third party APIs. Vervent validates, stores, and processes contact data within the Vervent Servicing Solution platform. Data is stored on database servers running Microsoft SQL Server within the production environment. All data is encrypted at rest, and SSL encrypts data in transit between the container and databases. Processed contact data is provided to customers in various ways:

- Customers can access the processed contact data via Vervent' online portals.
- Reports of processed contact data can be configured to send to customers via Vervent cloud-based email delivery platform, on a defined schedule.
- Outbound integrations via APIs send processed contact data to third-party marketing automating platforms, CRMs, and Custom Data Platforms.

Under a managed services agreement, Vervent manages the product 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. Vervent has a two-tiered Board structure to ensure additional oversight. An Operational Board meets with the management team on a weekly basis, or more frequently as needed. Management presents operational and third-party assessment results to the Board of Directors upon completion. In addition, a Holding Company Board provides oversight to the Company and has rights to appoint or terminate Operational Board Directors. Holding Company Board meetings occur annually and attendance is tracked, and discussion points and decisions are documented in Board minutes. Both Boards operate under bylaws that define responsibilities, including the oversight of management's system of internal control. The Holding Company 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.
- *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 Engineering team is

responsible for application development, initial testing of changes, and troubleshooting/resolving application issues.

- *Information Security* is responsible for 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 Servicing Solution 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 Servicing Solution platform, fielding customer calls regarding the Vervent Servicing Solution platform services, initiating and responding to help desk 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 Chief Information Security Officer who is responsible for the design and oversight of security initiatives. The CISO reports directly to the CTO. The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, and operation of the Vervent Servicing Solution platform. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CTO and CISO.

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.

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.

Monitoring of Subservice Organizations

The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively for any of Vervent's active, third-party subservice organizations, alone or in combination with controls at Vervent, to provide assurance that the required trust services in this report are met.

Third Party Subservice Organizations	
Criteria	**Control**
6.1	Vervent's third-party subservice organization is also responsible for logical access to the system and security measures to protect against threats from sources outside its system boundaries and the restriction of the transmission, movement, and removal of information to authorized internal and external users.
6.4	Vervent's third party subservice organization is also responsible for restricting physical access to the data center facilities, backup media, and other system components including network devices and servers.
7.2 & 7.3	Vervent's third party subservice organization is responsible for monitoring security activity logs regularly and monitors activity to maintain protection against malicious activity.
Vervent Management receives and reviews the subservice organization's SOC 2 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 the subservice organization to ensure that operations and controls expected to be implemented are functioning effectively.	

Complementary User Entity Controls and Responsibilities

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.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Description of Services Provided

Vervent technologies support management functions for loan, lease and credit card servicing:

- Vervent provides primary servicing functions for a variety of clients that include installment loans, leasing and servicing records utilizing Vervent's Servicing Solution (VSS) or the client's servicing platform.

The Vervent Servicing Solution (VSS) consists of the following components:

- Loan Module –provides full spectrum servicing functionality for loans and income share agreements to Vervent's clients.
- Lease Module –provides end-to-end lease lifecycle management to service Vervent's lease portfolios.
- Credit Card Module- provides a versatile card servicing platform with integrated application processing and full account lifecycle management.

Principal Service Commitments and System Requirements

Vervent's commitment to security covers consumers, clients and their customers and are documented and communicated to clients in the Master Services Agreement and the description of service document published on the customer-facing website. 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 Servicing Solution 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 at a Service Organization Relevant to Security 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 production systems.
- Prevent malware from being introduced to production systems.
- 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 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, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

Vervent regularly reviews security 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.