Information Security and Privacy Assessment

Assessment Risk Rating

Overall Rating	Cautious

Vendor	Service Provider, Inc.	Scope	Core Processing System and Services
Product	Core System		
Assessment Date	5/10/2021		
Function Provided	Core transaction processing		

venminder

Legend

Hover over section headings and data points to see the associated guidance and standards. A standard PDF viewer is required. Viewing within a browser disables this functionality. A printable reference document is attached at the end of this assessment.

YES	A positive or affirmative response to the control category was provided by the vendor.	–	A response was not provided to the control category by the vendor.
NO	A negative or insufficient response to the control category was provided by the vendor.	NA	The control category is not applicable to the scope of the assessment.

Rating Summary

🟠 **Risk Profile**	YES	*PII Data*	YES	*Cardholder Data*	NO	*Data Stored Outside the USA*

🟠 **Security Testing**	YES	*Penetration Testing Performed*	🟢 **Information Security**	NO	*Data is Encrypted*
	YES	*Defined Remediation Process*		NO	*Server/Network Security*
	YES	*Tested Within Last 12 Months*		YES	*Password Policies*
🟢 **Third-Party Reviews**	YES	*SOC Provided*	🟡 **Data Privacy**	YES	*Privacy Policy*
	YES	*SOC Unqualified*		YES	*Exempt Individual Data*
	YES	*Other Third-Party Audit Provided*		YES	*Breach Notification*
🟠 **Resiliency**	NO	*N+1 or Better Infrastructure*	🟡 **Physical Security**	YES	*Electronic Access Control*
	NO	*Monitoring/Maintenance*		YES	*Periodic Access Reviews*
	NO	*Backup Practices*		NO	*Security Cameras*
🟢 **Information Security Governance**	YES	*Information Security Policy*	🟢 **Business Continuity**	YES	*Vendor Maintains a BCP*
	NO	*Asset Management*		YES	*BCP Tested Annually*
	YES	*Employee/Contractor Security*		YES	*RTO and RPO*

Rating Summary Mapping and Methodology

Section Rating Summary Comments

• Vendor stated that Personally Identifiable Information (PII) is involved in the use of this product/service.

• Vendor stated that Cardholder Data (CHD) is involved in the use of this product/service.

• Vendor stated that they are required to comply with the European Union General Data Protection Regulation (GDPR), as well as the California Consumer Privacy Act (CCPA).

• While Vendor performs penetration testing annually, they stated that they do not perform Social Engineering Testing or Application Security Testing. Thus, the Security Testing section is rated High Risk.

• The following Physical Infrastructure Resiliency control(s) were noted as not in place: Redundant Generators, Redundant Cooling and Conditioning Systems, Redundant Uninterruptable Power Supplies, and Redundant Telecom Circuits. However, non-redundant implementations of these controls are in place at both Vendor's primary and secondary data center locations.

• The following Monitoring and Maintenance control(s) were noted as not in place: Generator Maintenance, UPS Maintenance, Cooling and Conditioning Maintenance, Network Monitoring, and Temperature and Humidity Monitoring.

• The following Backup Procedure control(s) were noted as not in place: Alternate Site Replication and Backups Sent Offsite Daily.

• Vendor stated they do not have a Software Asset Management Policy in place. However, Vendor noted that this is on their road-map for implementation in the next fiscal year.

• The following Encryption control(s) were noted as not in place: Encryption In-Transit.

• The following Server/Network Security control(s) were noted as not in place: DDoS Mitigation, Wireless Access Control, Network Segregation, and Web Application Firewall.

• Password Policy for Client's Customer Access is considered out of scope as Customers do not have access to this product/service.

• Vendor does not have Data Center Security Cameras in place.

Preface

This assessment identifies key risks to your organization's operations, assets, and customers, posed by current and potential vendors. Each control within this assessment ties back to relevant industry guidance and standards addressing vendor risk, allowing key decision makers to confidently weigh vulnerabilities introduced by vendors and respond to the resulting risks. This assessment allows you to identify whether the vendor is providing an acceptable service relating to cybersecurity, privacy, resiliency, physical security, and business continuity.

This assessment was developed using the following industry guidance and standards.

Code of Federal Regulations Title 12 – Part 30 for OCC, Part 225 for FRB, Part 364 for FDIC, Part 748 for NCUA	12CFR-*.* | 12CFR-III.D.1,2
OCC 2005-1/2005-13/2011-26	OCC20**-*.*
FFIEC IT Examination Handbook – Outsourcing Technology Services	OT.*.*
FFIEC IT Examination Handbook – Information Security Booklet	IS.*.*
FFIEC IT Examination Handbook – Business Continuity Booklet	BCP.*.*
FFIEC IT Examination Handbook – Management Booklet	MGT.*.*
FFIEC IT Examination Handbook – Operations Booklet	OP.*.*
FFIEC IT Examination Handbook – Audit Booklet	AUD.*.*
FFIEC IT Examination Handbook - Wholesale Payment Systems Booklet	WPS.*.*
SEC Regulation SCI reference to NIST 800-53 Rev. 4	800-53-*.*
FINRA Report on Cybersecurity Practices	FINRA-pg*
Center for Internet Security – Critical Security Controls	CSC-*
New York Department of Financial Services 23 NYCRR 500	NYCRR-*
Health Insurance Portability and Accountability Act	HIPAA-*
EU General Data Protection Regulation	GDPR-*
California Consumer Privacy Act	CCPA-*
AICPA Trust Services Criteria	TSC-*
NIST Framework for Improving Critical Infrastructure Cybersecurity version 1.1	CSF.*
ISO/IEC 27001:2013	ISO.*

Risk Profile

HIGH

Types of customer data involved with this product:

YES	Name	YES	Date of Birth	YES	Account Number(s)
YES	Address	YES	Social Security Number	YES	Cardholder Data (CHD)
NO	Telephone Number	NO	Driver's License Number	NO	Protected Health Information (PHI)
YES	Email Address	NO	Taxpayer Identification	NO	Other (Please Specify)

Types of client data involved with this product:

YES	Internal Policies/Documentation	NO	Non-Public Product/Service Information
YES	Non-Public Business Plans	NO	Other (Please Specify)
YES	Non-Public Financial Information		

Experience with the function outsourced:

Twenty-three (23) years.

Critical subservice organizations:

None noted.

Client data stored outside the USA:	NO
Services provided from outside the USA:	NO

Product hosted/installed:

□ Client Location

☑ Vendor Location

□ Subservice Location

Security Testing

HIGH

Penetration tests are performed by internal staff	NO
Penetration tests are performed by a third party	YES
Date of the most recent test	7/22/20

Scope of penetration testing

Externally-facing networks.

Frequency of penetration testing

Annually

If other:

Medium and higher findings are remediated timely	YES
Planned remediation date from last test	NA
Results were reviewed by senior management	YES

Social engineering or phishing performed	NO

Frequency of social engineering testing

No Testing Performed

If other:

Application security tests are performed by internal staff	NO
Application security tests are performed by a third party	NO
Medium and higher findings are remediated timely	NO
Planned remediation date from last test	–
Results were reviewed by senior management	NO

System and Organization Controls (SOC) Report
(formerly Service Organization Control)

10/1/19 Through 9/30/20

	YES	NO
A Bridge/Gap letter was provided.	☑	□
A Bridge/Gap Letter for the period of Audit End Date through Bridge Letter Date states that there have been no material changes to the control environment.	☑	□

Type of SOC Report: SOC 2 Type II

Services in scope

Core Processing System and Services

	YES	NO
SOC report qualified	□	☑

NA - Opinion unqualified.

Exceptions

There were no exceptions or deviations noted within the report ☑

Exception 1	Control #	Page #	Exception 8	Control #	Page #
Exception 2	Control #	Page #	Exception 9	Control #	Page #
Exception 3	Control #	Page #	Exception 10	Control #	Page #
Exception 4	Control #	Page #	Exception 11	Control #	Page #
Exception 5	Control #	Page #	Exception 12	Control #	Page #
Exception 6	Control #	Page #	Exception 13	Control #	Page #
Exception 7	Control #	Page #	Exception 14	Control #	Page #

Payment Card Industry (PCI) Attestation of Compliance (AOC)

Documented assessment completed on 12/1/20

Services in scope

Core Processing System and Services

Compliance status marked compliant ☑

Qualified Security Assessor Performed the Assessment and Signed the AOC ☑

HIPAA HITRUST Certified Security Framework (CSF)

Certification Date

Authorized External Assessor Validation □

Compliance status marked compliant □

Services in scope

Not required as PHI is not in scope.

ISO/IEC 27001

Revision

Not required as Vendor provided a SOC report instead.

Original Issue Date

Issue Date

Expiration Date

Services in scope

Other

Type

SOC 1 Type II report

Revision

10/1/19 through 9/30/20

Original Issue Date

Issue Date

Services in scope

Core Processing System and Services

Resiliency

HIGH

The following resiliency controls or better are in place for Vendor's primary data center.

NO	Generator – N+1
NO	Cooling and Conditioning – N+1
NO	Uninterruptable Power Supplies – N+1
NO	Multiple telecom circuits with failover capacity

The following system monitoring and supporting controls are in place.

YES	Fire Detection	YES	Fire System Maintenance
YES	Fire Suppression	NO	Cooling and Conditioning System Maintenance
NO	Generator Maintenance	NO	Network Monitoring
NO	Uninterruptable Power Supply Maintenance	NO	Temperature and Humidity Monitoring

The following data resiliency controls are in place for production data.

YES	Onsite Backups	YES	Monitored Alerts on Failed Backups
YES	Backups Tested Annually	NO	Alternate Site Replication
YES	Offsite Backups	NO	Backups Sent Off-site Daily

Information Security Governance

LOW

Formal Programs or Policies

YES	Information Security
YES	Incident Management
NO	Log Management
YES	Change Management
NO	Risk Management
YES	Asset Management - Hardware
NO	Asset Management - Software
YES	Vendor Management/Due Diligence
YES	Logical Access Management
YES	Data Destruction Post-Contract

Represented Practices

YES	Data Classification
YES	Media Sanitization
YES	Separation of Duties
NO	Principle of Least Privilege
YES	Employee/Contractor Background Checks
YES	Employee/Contractor Security Training
YES	Annual Board or Appropriate Committee Involvement
YES	Designated Chief Information Security Officer (CISO)
YES	Logical Access Review/Termination
YES	Patch Management

Information Security

LOW

YES Encryption At-Rest

NO Encryption In-Transit

YES Backup Media Encrypted

YES IDS/IPS

NO DDos Mitigation

NO Wireless Access Control

NO Network Segregation

YES Secure Device Baselining

YES Antimalware

YES Ongoing Vulnerability Assessments

YES Remote Access Requires Multifactor Authentication

YES Event Log Correlation and Analysis

Type of connection or method of file transfer (Client<->Vendor)

VPN

If other:

Type of connection (Customer<->Vendor)

No Customer access

If other:

Vendor Software/Application

NO Web Application Firewall in place

YES Designated security personnel involved in SDLC

YES Security testing is a part of build verification

YES Third parties do not maintain access to dev/prod

YES Multifactor authentication for administrative access

YES Multifactor authentication available for client

NA Multifactor authentication available for customer

NA Complex device identification

Password policy for employee access

Minimum length

Eight (8) characters

Character sets available

YES ABC YES abc YES 123 YES !@#

Required number of used character sets

Four (4) sets

Max age

Ninety (90) days

Password policy for client access

Minimum length

Eight (8) characters

Character sets available

YES ABC YES abc YES 123 YES !@#

YES Single-Sign-On available for client access

Required number of used character sets

Three (3) sets

Max age

Sixty (60) days

Password policy for customer access

Minimum length

NA - No Customer access

Character sets available

NA ABC NA abc NA 123 NA !@#

NA Single-Sign-On available for customer access

Required number of used character sets

NA - No Customer access

Max age

NA - No Customer access

Data Privacy

MEDIUM

YES	Provides Notice to Data Subjects About Its Privacy Practices
NO	Data Protection Officer
NO	Maintains a Data Privacy Code of Conduct
YES	Collects Accurate, Up-to-Date, Complete, and Relevant PII
YES	Able to Display an Individual's Data and Who It's Shared With
YES	Able to Export an Individual's Data in a Common Format
NO	Able to Update/Correct an Individual's Data
YES	Able to Exempt an Individual's Data from Sharing/Selling
NO	Able to Delete an Individual's Data
YES	Able to Delete or Return all PII at Contract Termination
NO	Persons Interacting with Sensitive Data Sign a Confidentiality Agreement
YES	Persons Interacting with Sensitive Data Receive Privacy Training
NO	Data is Only Used for Contracted Purpose of the Controller
YES	Data is not Shared with a Fourth Party without Controller Consent
YES	Records of Processing Activities are Maintained
NO	Client Audit Cooperation
YES	Data Breach Notification/Unauthorized Disclosures of PII are Tracked
NO	Data is Pseudonymized/De-Identified
NO	Data is Masked where Appropriate

Physical Security

MEDIUM

Data Center Location(s)

Louisville, Kentucky (Primary)
Charlotte, North Carolina (Disaster Recovery Hot site)

Access Controls

The following access controls were addressed through response or evidence:

YES	Electronic Access Control
NO	Multifactor Authentication
YES	Access is Reviewed
YES	Visitor Tracking
NO	Security Guards
NO	Camera System

Business Continuity

LOW

YES Vendor has documented Business Continuity and Disaster Recovery Plans (BCP) to recover to normal operations

YES Board of Directors or Senior Management provides oversight of the BCP

YES Plans undergo ongoing maintenance

YES Plans are updated following impacting process/provider changes

Plans are a part of internal or external audits/assessments

☑ Internal ☐ External

The following types of scenarios are planned for

☑ Pandemic ☑ Loss of office availability

☐ Loss of critical subservice

☐ Other (Please Specify)

YES Documented process for client notification for service interruption or degradation

Briefly describe

Client services will notify via phone and email.

YES A Business Impact Analysis is performed

Recovery Time Objective (RTO) and Comments	Tested and Met
One (1) hour	☑

Recovery Point Objective (RPO) and Comments	Tested and Met
Twenty-four (24) hours	☑

NO Plans rely on subservice organization(s)

NA Plans were developed in coordination with subservice organization(s)

NA Testing has occurred with subservice organization(s)

NA Vendor has reviewed subservice organization(s) BCP

YES Plans cover all offices and data centers

YES A dedicated team is focused on BCP and DR

NO A third party is used for planning

An alternate Vendor-owned office facility is available

Configuration	Capacity
Warm	Full

NO Staff can operate remotely

An alternate Vendor-owned data center is available

Configuration	Capacity
Hot	Full

YES Distance between primary and alternate locations is great enough that a disaster in one location does not also impact the other

YES Both IT and Business Unit staff are included in BC/DR testing

	Frequency of testing	Last tested	Remediated
BCP	Annually	6/20/20	8/30/20
DRP	Annually	9/30/20	11/15/20

The following types of tests are performed

☑ Tabletop ☐ Simulation

☑ Functional Drill ☐ Full Interruption

NO Clients can participate in BCP tests

Complementary User Entity Controls

Certain control objectives specified in the Third Party Reviews can only be achieved if your organization is in compliance with the complementary user entity controls listed in the applicable report. If this review is for a subservice provider of one of your direct vendor relationships, you should ensure that your vendor is adhering to these controls as a part of their vendor management program.

The complementary user entity controls found within the SOC report(s) used to perform this assessment have been provided separately.

Additional Report Comments

It should be noted that it is the responsibility of the Board of Directors to determine whether the organization agrees with the opinion-based risk levels expressed in this report.

Prepared By

Sarah B. Sample, CRVPM, CISSP

Senior Information Security Specialist

Venminder, Inc.

Sarah B Sample

Rating Explanation

Rating	Explanation
LOW	Vendor appears to maintain a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear appropriate.
MEDIUM	Vendor appears to maintain a partially well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear satisfactory.
HIGH	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a cautionary level of risk.
SEVERE	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a severe level of risk.

Standard and Regulation References

Documentation Utilized

- 2020 Core Processing SOC 1 and 2 GAP Letter
- 2020 Core Processing SOC 1 Type II
- 2020 Core Processing SOC 2 Type II
- Business Continuity Program Summary
- Compliance Statement
- Core Vendor Assessment Statement
- Corporate Security Policy
- Cyber Response
- Data Loss Prevention Statement
- Enterprise Resilience Policy
- Executive Summary
- Information Security Assessment Questionnaire
- Network Defense Statement
- Pen Test Statement
- Standard Information Gathering (SIG) Questionnaire - Core
- Third Party Management
- PCI Attestation of Compliance
- Privacy Policy