



Data Protection Assessment

Assessment Risk Rating

Overall Rating

Vendor

Scope

Product

Assessment Date



Function Provided








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.
- NO** A negative or insufficient response to the control category was provided by the vendor.

- A response was not provided to the control category by the vendor.
- NA** The control category is not applicable to the scope of the assessment.

Rating Summary

 Risk Profile <ul style="list-style-type: none"> PII Data Cardholder Data Data Stored Outside USA 	
 Information Security Governance <ul style="list-style-type: none"> Information Security Program Asset Management Employer/Contractor Security 	 Resiliency <ul style="list-style-type: none"> Backup Practices Infrastructure Resiliency Monitoring/Maintenance
 Information Security <ul style="list-style-type: none"> Data is Encrypted Server/Network Security Penetration Testing Performed 	 Physical Security <ul style="list-style-type: none"> Electronic Access Control Periodic Access Reviews Security Cameras
 Data Privacy <ul style="list-style-type: none"> Privacy Policy Exempt Individual Data Breach Notification 	 Business Continuity <ul style="list-style-type: none"> Vendor Maintains a BCP BCP Tested Annually RTO and RPO



Rating Summary Mapping and Methodology

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 Article 32	GDPR-*
California Consumer Privacy Act	CCPA-*
AICPA Trust Services Criteria	TSC-*
NIST Framework for Improving Critical Infrastructure version 1.1	CSF.*
ISO/IEC 27001:2013	ISO.*

Venminder Assessment Overview

Additional Comments:

Recommendations



Risk Profile

Types of customer data involved with this product:	Name	Date of Birth	Account Number(s)
	Address	Social Security Number	Cardholder Data (CHD)
	Telephone Number	Driver's License Number	Protected Health Information
	Email Address	Taxpayer Identification	Other (Please Specify)

Types of client data involved with this product:	Internal Policies/Documentation	Non-Public Product/Service Information
	Non-Public Business Plans	Other (Please Specify)
	Non-Public Financial Information	

Experience with the function outsourced:

Critical subservice organizations:

Client data stored outside the USA

Product hosted/installed:

Client Location

Services provided from outside the USA

Vendor Location

Subservice Location

The following Privacy Regulations are applicable to Vendor:



Information Security Governance

Information Security Program

Incident Management

Vendor Management/Due Diligence

Asset Management - Hardware

Asset Management - Software

Logical Access Management and Review

Principle of Least Privilege

Background Screening

Security Training

Annual Board of Directors Involvement

Qualified Chief Information Security Officer (CISO)



Information Security

Security Incident and Event Management (SIEM)
Encryption In-Transit
Encryption At-Rest
Secure Device Configuration and Maintenance
Security Appliances
Wireless Access Control
Administrative Access Requires MFA
Remote Access Requires MFA

MFA available for Client
Third Parties do not Maintain Access to Dev/Prod
Penetration Testing Performed by Qualified Personnel
Application Security Testing Performed by Qualified Personnel
Weekly Vulnerability Scans
Documented Vulnerability Remediation Plan
Social Engineering Testing



Data Privacy

Provides Notice to Data Subjects About its Privacy Practices
Data Protection Officer
Maintains a Data Privacy Code of Conduct
Collects Accurate, Up-to-Date, Complete, and Relevant PII
Able to Display an Individual's Data and Who It's Shared With
Able to Export an Individual's Data in a Common Format
Able to Update/Correct an Individual's Data
Able to Exempt an Individual's Data from Sharing/Selling
Able to Delete an Individual's Data
Able to Delete or Return all PII at Contract Termination

Persons Interacting with Sensitive Data Sign a Confidentiality Agreement
Persons Interacting with Sensitive Data Receive Privacy Training
Data is Only Used for Contracted Purpose of the Controller
Data is not Shared with a Fourth Party without Controller Consent
Records of Processing Activities are Maintained
Client Audit Cooperation
Data Breach Notification-Unauthorized Disclosures of PII are Tracked
Data is Pseudonymized/De-Identified
Data is Masked where Appropriate



Resiliency

Onsite Backups
Offsite Backups or Replication
Backup Monitoring and Testing
Generators
Uninterruptable Power Supplies

Cooling and Conditioning System
Fire Detection and Suppression System
Redundant Telecommunication Links
Monitoring and Maintenance of Environmental and Power Systems



Physical Security

Electronic Access Control
Access is Reviewed
Security Guards

Camera System
Visitor Tracking



Business Continuity

Documented Business Continuity and Disaster Recovery Plans (BC/DR)
Board of Directors Oversight
Ongoing Maintenance of BC/DR Plans
Plans Cover Work Area Recovery
Plans Cover Data Center Recovery
Plans Ensure Geographic Resilience to Localized Events
A BIA Is Performed and Maintained

Recovery Time Objective (RTO) and Comments

Recovery Point Objective (RPO) and Comments

Frequency of BCP Testing
Frequency of DRP Testing

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

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