Information Security & Privacy Assessment

IT Cloud Provider | Cloud Hosting

vendiligence™

Vendor Profile

IT Cloud Provider

Product
Cloud Hosting

Assessment Date
11/17/2023

Service Description
The Vendor was noted as providing the following service(s): IT Cloud Provider - Cloud Hosting

Domain URL
itcloudprovider.com

Vendor Type/Industry
Cloud Hosting Infrastructure

Vendiligence™ Overall Rating

SATISFACTORY

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.

Vendor Inherent Risk Profile Summary

Risk Summary Rating
HIGH

YES Personally Identifiable Information (PII)

YES Protected Health Information (ePHI)

YES Cardholder Data (CHD)

YES Client Data

Section Rating Summary

Data Privacy LOW	**Security Testing** LOW	**Third-Party Reviews** MEDIUM	**Information Security Governance** MEDIUM
Sensitive Data Security MEDIUM	**Resiliency** LOW	**Business Continuity** LOW	

Report Comments and Recommendations

Vendor stated that Personally Identifiable Information (PII), Card Holder Data (CHD), and Protected Health Information (ePHI) is involved in the use of this product/service. Client is encouraged to request evidence that Vendor has a documented Third Party Vendor Management/Due Diligence program in place. Client is encouraged to request evidence that Vendor has a documented PII Retention Policy in place as well as someone in leadership acting in the capacity of Chief Information Security Officer. Vendor did not provide adequate evidence that data is encrypted in transit or at rest. Client is encouraged to request documentation surrounding current encryption methods. Client is encouraged to request information surrounding the following data security controls we would expect to see: DDOS Mitigation, Wireless Access Controls, Data Classification, Media Sanitization, Breach Notification, Environment Segmentation, Environment Segmentation, and MFA for administrative access. Client is encouraged to request evidence that environmental equipment is properly maintained and serviced regularly.

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Information Security & Privacy Assessment

IT Cloud Provider | Cloud Hosting

vendiligence™

Legend			
	A positive or affirmative response to the control category was provided by the vendor.	N/P	A response was not provided to the control category by the vendor.
	A negative or insufficient response to the control category was provided by the vendor.	N/A	The control category is not applicable to the scope of the assessment.

Risk Profile	Regulation Mapping	HIGH

Type of customer/consumer data involved in this product:

YES Name	YES Date of birth	YES Account Number(s)
YES Address	YES Social Security Number	YES Cardholder Data (CHD)
YES Telephone Number	YES Drivers License Number	YES Personally Identifiable Information (PII)
YES Email Address	YES Taxpayer Identification	YES Protected Health Information (ePHI)
		Other (please specify) N/A

Type of client data involved with this product:

NO Internal Policies/Documentation	NO Non-Public Product/Service Information
YES Non-Public Business Plans	Other Types of Client Data (please specify)
YES Non-Public Financial Information	Employee Records

Experience with the function outsourced: 13 Years

Critical Subservice Organizations and services provided

ServiceCore - Provides call center and consumer services

NO Client data stored outside the USA

NO Services provided from outside the USA

Product hosted/installed: ☑ Vendor Location

Assessment Of Controls

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.

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Information Security & Privacy Assessment

IT Cloud Provider | Cloud Hosting

Data Privacy

Regulation Mapping

LOW

- YES — Provides notice to data subject about its privacy practices
- N/P — Data Protection Officer
- YES — Obtains consent from data subjects where required
- 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
- YES — Able to Update/Correct an Individual's Data
- YES — Able to Exempt an Individual's Data from Sharing/Selling
- YES — Able to exempt an individual from automated decisions
- YES — Able to delete an individual's data
- YES — Able to delete or return all PII at contract termination
- YES — Process in place for handling privacy requests (DSARS)
- YES — Vendor maintains a data privacy code of conduct
- YES — Persons interacting with sensitive data sign a confidentiality agreement
- YES — Persons interacting with sensitive data receive privacy training
- YES — Data is only used for contracted purpose
- YES — Data is not shared with a fourth party without consent
- N/P — Records of processing activities are maintained
- YES — Vendor allows for full cooperation in audits for clients
- YES — Data breach notification/unauthorized disclosures of PII are tracked
- YES — Data is pseudonymized/de-identified
- YES — Data is masked where appropriate

Security Testing

Regulation Mapping

LOW

- NO — Penetration tests are performed by internal staff
- YES — Penetration tests are performed by a third party

Date of most recent penetration test: 2/1/2023

Scope of penetration testing: Core Network

Frequency of penetration testing: Quarterly

Frequency of penetration testing (other): N/A

- YES — Any Medium or higher findings identified during the penetration tests are remediated timely

Planned remediation date from last penetration test: 8/31/2023

- NO — Application security tests are performed by internal staff
- YES — Application security tests are performed by a third party

Date of most recent application test: 2/10/2023

Scope of application security testing: IT Cloud Provider Service Application

Frequency of application security testing: Quarterly

Frequency of application security testing (other): N/A

- YES — Any Medium or higher findings identified during the application tests are remediated timely

Planned remediation date from last application test: 8/31/2023

- YES — Vulnerability scans/tests are performed by internal staff
- YES — Vulnerability scans/tests are performed by a third party

Date of most recent vulnerability test: 7/1/2023

Scope of vulnerability scans/tests: N/P

Frequency of vulnerability scans/tests: Daily

Frequency of vulnerability scans/tests (other): N/A

- YES — Any Medium or higher findings identified during the vulnerability tests are remediated timely

Planned remediation date from last vulnerability test: 7/7/2023

- YES — Social engineering or phishing performed

Frequency of social engineering tests: Monthly

Frequency of social engineering tests (other): N/A

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Third-Party Reviews

Regulation Mapping | MEDIUM

System and Organization Controls (SOC) Report

4/1/2022 through 3/31/2023

Type of SOC Report: SOC 2 Type II

Services in Scope of SOC Report: VenCore Product

SOC Report Opinion: Unqualified

A Bridge/Gap letter was provided: Yes

A Bridge/Gap Letter for the period of the Audit End Date through Bridge Letter Date states that there have been no material changes to the control environment: Yes

YES Were there any exceptions found within the report?

Number of exceptions: 1-5

Exceptions

Exception Details:

- Two (2) Exceptions found -
- Exception 1 -CC8.1.1 - Page 106
- Exception 2 - CC11.2.3 - Page 121

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

Services in scope of PCI AOC assessment: Credit Card Processing for IT Cloud Provider application services

YES PCI AOC compliance status marked compliant

YES Qualified Security Assessor Performed the Assessment and signed the AOC

Date of PCI AOC assessment completion: 2/28/2023

HIPAA HITRUST Certified Security Framework (CSF)

HIPAA certification services in scope: IT Cloud Provider EMR add on application

YES HIPAA authorized external assessor validation

YES HIPAA compliance status marked compliant

HIPAA Certification Date: 12/31/2022

ISO/IEC 27001

ISO/IEC 27001 Services in Scope: N/A

ISO/IEC 27001 Revision: N/A

ISO/IEC 27001 original issue date: N/A

ISO/IEC 27001 expiration date: N/A

ISO/IEC 27001 issue date: N/A

Other

Type (other): N/A

Original issue date (other): N/A

Services in scope (other): N/A

Issue date (other): N/A

Revision date (other): N/A

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Information Security Governance

Regulation Mapping

MEDIUM

Formal Programs or Policies

- YES Information Security
- YES Incident Management
- YES Change Management
- YES Risk Management
- YES Mobile Device/BYOD
- YES Asset Management - Hardware
- YES Asset Management - Software
- NO Vendor Management/Due Diligence
- YES Client Data Destruction Post-Contract
- YES Evidence of Insurance

Represented Practices

- YES Employee/Contractor Background Checks
- NO PII Retention Policy
- YES Employee/Contractor Security Training
- YES Board/Executive/Senior Management Involvement
- NO Designated Chief Information Security Officer (CISO)
- YES Patch Management

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Sensitive Data Security	Regulation Mapping	MEDIUM

N/P Encryption at Rest	NO Wireless Access Control	NO Media Sanitization
N/P Encryption in Transit	YES Secure Device Baselining	YES Principle of Least Privilege
YES Logical Access Management	YES Remote Access Requires Multifactor Authentication	YES Separation of Duties
NO DDoS Mitigation	NO Data Classification	

Incident Detection and Response	YES IDS/IPS	NO Breach Notification
	YES Event Log Correlation and Analysis	YES Periodic Logical Access Review/Termination
	YES Network Segmentation	
	YES Antimalware	
Vendor Software/Application Security	YES Web application firewall	YES Third parties do not maintain access to dev/prod
	YES Designated security personnel involved in SDLC	NO Production and development environment segmentation
	YES Security testing is part of build verification	
Password Policy For Employee Access	YES Does vendor require appropriate complexity/length/unpredictability for employee passwords?	NO Multifactor authentication for administrative access
	YES Does policy require employee to change from the default password?	
Password Policy For Client Access	YES Does vendor require appropriate complexity/length/unpredictability for client passwords?	YES Multifactor authentication available for client access
	YES Does policy require client to change from default password?	YES Single-Sign-On available for client access
Password Policy For Customer/Consumer Access	YES Does vendor require appropriate complexity/length/unpredictability for customer/consumer passwords?	YES Multifactor authentication available for customer/consumer access
	YES Does policy require customer/consumer to change from the default password?	YES Single-Sign-On available for customer/consumer access

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Resiliency		Regulation Mapping	LOW
The following resiliency controls or better are in place for Vendor's primary data center	YES Generators (with redundancy) YES Cooling & Conditioning System (with redundancy)	YES Uninterruptable Power Supplies (with redundancy) YES Redundant Internet Connectivity	
The following system monitoring and supporting controls are in place	YES Fire Detection YES Fire Suppression NO Generator Maintenance NO Uninterruptable Power Supply Maintenance	YES Fire System Maintenance NO Cooling & Conditioning System Maintenance YES Network Monitoring YES Temperature and Humidity	
The following data resiliency controls are in place for production data	YES Primary Site Backups Primary Site Backup Frequency Nightly Primary Site Backup Type Full YES Offsite/Offline Backups Offsite/Offline Backup Frequency Nightly Offsite/Offline Backup Type Full YES Backups Tested Annually	YES Monitored Alerts on Failed Backups YES Alternate Site Replication NO Backup Media Encrypted	
Physical Security	YES Electronic Access Control YES Multifactor Authentication for Physical Access YES Physical Access is Reviewed	YES Visitor Tracking NO Security Guards YES Camera System	

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Business Continuity

Regulation Mapping | LOW

Overview

YES Vendor has documented Business Continuity Plan (BCP)

YES Vendor has documented Disaster Recovery Plan (DRP)

NO Board of Directors or Senior Management provides oversight of the BCP

YES Plans cover all offices and data centers

YES A dedicated team is focused on BC and DR

YES Plans undergo ongoing maintenance

YES Plans are updated with any significant organization changes

Plans are part of internal or external audits/internal or external assessments

Both

YES BCP includes a specific Pandemic Plan

The following types of scenarios are planned for:

- [x] Loss of office availability, Loss of critical subservice

The following types of scenarios are planned for (other):

Environmental, Pandemic, and system outages

YES Documented process for client notification for service interruption or degradation

Briefly describe documented process for service interruption or degradation

Vendor provided a documented step by step service interruption plan that includes a call tree, POCs and actionable steps to continue to deliver service through an interruption. The plan is distributed and available to all necessary groups and is review upon hiring (for applicable roles) and re-reviewed and signed off on annually. The plan is also includes notification parameters as appropriate.

Business Continuity Plan Testing

N/P A Business Impact Analysis is performed

YES RTO Tested and Met

Recovery Time Objective (RTO) and Comments >72 hours

YES RPO Tested and Met

Recovery Point Objective (RPO) and Comments >72 hours

YES Employees have the ability to work at full capacity remotely or have an alternate facility

NO Vendors BCP relies on a subservice for Data Center Recovery

N/A Vendor's Data Center Recovery plans were tested with subservice organization(s)

N/A Vendor's Data Center Recovery plans were developed in coordination with subservice organization(s)

N/A Vendor has reviewed Data Center Recovery subservice organization(s) BCP

YES Vendor's BCP relies on a subservice for Office Space Recovery

YES Vendor's Office Space Recovery plans were developed in coordination with subservice organization(s)

YES Vendor's Office Space Recovery plans were tested with subservice organization(s)

YES Vendor has reviewed Office Space Recovery subservice organization(s) BCP

YES BCP/DRP offline access

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

YES Are employees trained on Business Continuity and Disaster Recovery

	Frequency of testing	Last tested	Remediated
BCP	Annually	2/10/2023	5/3/2023
DRP	Annually	2/10/2023	5/3/2023

The following types of BCP tests are performed

- [x] Tabletop, Simulation, Full interruption

Frequency of BCP testing (other) N/A

The following types of DRP tests are performed

- [x] Tabletop, Simulation, Full Interuption

Frequency of DRP testing (other) N/A

YES Distance between primary and alternate locations is appropriate

An alternative data center is available with the configuration of

Warm

NO Clients can participate in BCP tests

Vendor utilizes the following for personnel recovery

Transitions to remote work

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Documents Utilized

- LogicalAccess Policy.pdf
- VRP_2023.pdf
- BCA_program_plan.pdf
- DR_test_09302022.pdf
- RTO.RPO Guide.pdf
- SOC 2 Type II_10312022.pdf
- ISPA.Questionairre.072023
- Incident Resp plan_08.2022.pdf
- Pen_Test_Exec Summ Q3.pdf
- InformatioSecProgram.pdf
- COI 2022_2023.pdf
- Technology GCC_2022_SECURED.pdf
- SIG_Core 2022.pdf

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Disclaimer

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 level expressed in this report.

All information contained in this assessment is the work product of the Venminder, Inc. Information Security Operations Team. Documents listed as Resources Utilized have been reviewed and assessed by an Information Security Subject Matter Expert and this assessment has been reviewed and approved for distribution. For more information on Venminder's Subject Matter Experts, please click here.

The objective of this Assessment is to assess a third party's general controls relating to their ongoing ability to protect data and deliver the products and services for which you have contracted. This assessment is not intended for, nor should it be used for, the purpose of assessing the third party's likelihood of suffering a data breach, attack, or other business impacting event causing the inability to provide contracted services, nor as a guarantee the vendor will follow any assessed plan or meet specified objectives. This Assessment is intended solely for the information and use by the client and is not intended to be and should not be used by anyone else other than the objectives listed herein.

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.

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

Industry Guidance and Standards Utilized

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

INDUSTRY GUIDANCE AND STANDARDS	MAPPING REFERENCE
AICPA Trust Services Criteria	TSC-*
California Consumer Privacy Act	CCPA-*
California Privacy Rights Act	CPRA.**
Canadian Personal Information Protection and Electronic Documents Act	PIPEDA.*
Center for Internet Security - Critical Security Controls v8	CSC-*
China Personal Information Protection Law	PIPL.*
Colorado Privacy Act	CPA.**
Connecticut Data Privacy Act	CTDPA.**
EU General Data Protection Regulation	GDPR-*
FFIEC IT Examination Handbook - Wholesale Payment Systems Booklet	WPS.**
FFIEC IT Examination Handbook - Audit Booklet	AUD.**
FFIEC IT Examination Handbook - Business Continuity Booklet	BCP.**
FFIEC IT Examination Handbook - Information Security Booklet	IS.**
FFIEC IT Examination Handbook - Management Booklet	MGT.**
FFIEC IT Examination Handbook - Operations Booklet	OP.**
FFIEC IT Examination Handbook - Outsourcing Technology Services	OT.**
FINRA Report on Cybersecurity Practices	FINRA-pg*
Health Insurance Portability and Accountability Act	HIPAA-*
Interagency Guidelines Establishing Information Security Standards	12CFR-**
Interagency Guidance on Third-Party Relationships (Board, FDIC, & OCC) 06.2023	TPRM.*
ISO/IEC 27001:2022	ISO.*
New York Department of Financial Services - 23 NYCRR 500	NYCRR-*
NIST Framework for Improving Critical Infrastructure Cybersecurity version 1.1	CSF.*
NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations	800-53-r5-**
NIST SP 800-63b Digital Identity Guidelines	800-63b.**
OCC 2021-36	OCC20**-**
OSFI B-10 Third-Party Risk Management	OSFI-B-10-****
OSFI B-13 Technology and Cyber Risk Management	OSFI-B-13-****
SEC Regulation SCI reference to NIST 800-53 Rev. 4	800-53-**

© Venminder, Inc. All Rights Reserved. Confidential

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.