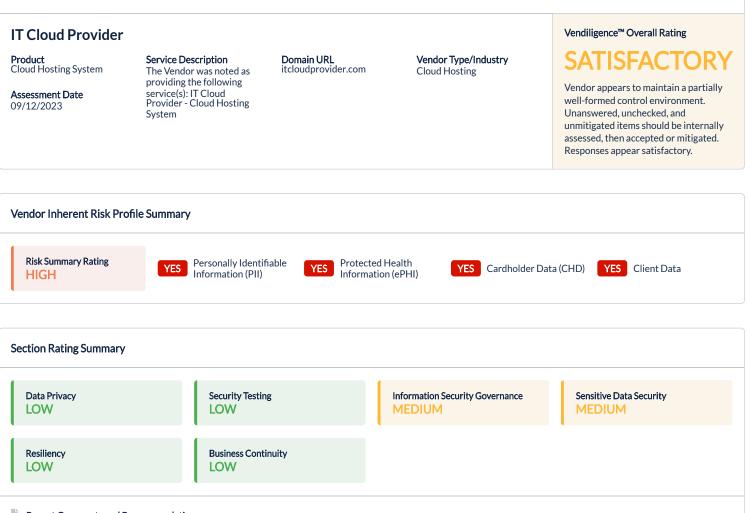
IT Cloud Provider | Cloud Hosting System

Evendiligence™





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 a 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, and MFA for administrative access. Client is encouraged to request evidence that environmental equipment is properly maintained and serviced regularly.



Page 1/7

IT Cloud Provider | Cloud Hosting System



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	<mark>₽</mark> HIGH
	YES Na	ame	YES Date of birth	YES A	account Number(s)
	YES Ac	ldress	YES Social Security Nu	umber YES C	Cardholder Data (CHD)
Type of customer/consumer data involved in this product:	YES Te	lephone Number	YES Drivers License N		ersonally Identifiable nformation (PII)
nivolveu in this product.	YES En	nail Address	YES Taxpayer Identific		Protected Health Information PHI)
				Other (ple	ease specify) NA
		ternal licies/Documentation	NO Non-Public Produ	ict/Service	
Type of client data involved with this product:	t data involved with this YES N		Other Types of Client Data specify)	a (please	
		on-Public Financial formation	Employee Records		
Experience with the function outsourced	13 years	NO Client data stored	outside the USA	Product hosted/install	ed 🛛 Vendor Location
Critical Subservice Organizations and services provided		NO Services provided from outside the USA			
ServiceCore - Provides call center and conservices	nsumer				

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.

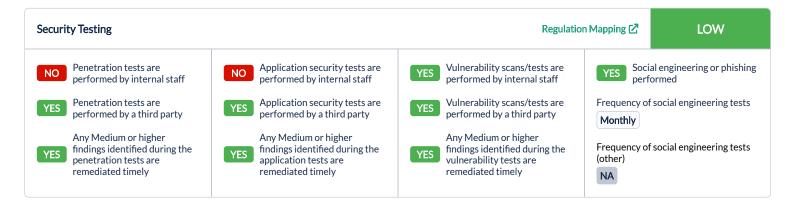


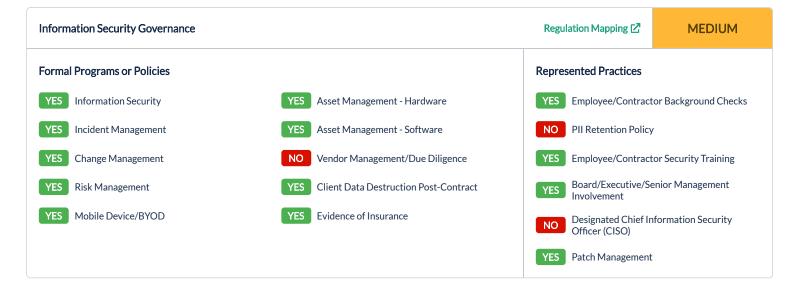
Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Venminder, Inc. and not eligible for redistribution without expressed written permission from Venminder, Inc.

IT Cloud Provider | Cloud Hosting System

≣vendiligence™

Data Privacy		Regulation Mapping 🖸	LOW
YES Provides notice to data subject about its privacy practices	YES Able to exempt an individual from automated decisions	YES Data is not shared wi	th a fourth party without
N/P Data Protection Officer	YES Able to delete an individual's data	N/P Records of processin	g activities are maintained
YES Obtains consent from data subjects where required	YES Able to delete or return all PII at contract termination	YES Vendor allows for ful clients	l cooperation in audits for
YES Collects Accurate, Up-to-Date, Complete, and Relevant PII	YES Process in place for handling privacy requests (DSARS)	YES Data breach notificat disclosures of PII are	
YES Able to Display an Individual's Data and Who It's Shared With	YES Vendor maintains a data privacy code of conduct	YES Data is pseudonymiz	ed/de-identified
YES Able to Export an Individual's Data in a Common Format	YES Persons interacting with sensitive data sign a confidentiality agreement	YES Data is masked wher	e appropriate
YES Able to Update/Correct an Individual's Data	YES Persons interacting with sensitive data receive privacy training		
YES Able to Exempt an Individual's Data from Sharing/Selling	YES Data is only used for contracted purpose		





© 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.

IT Cloud Provider | Cloud Hosting System

Evendiligence[™]

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 Privil	ege
YES Logical Access Management	YES Remote Access Requires Multifactor Authentication	YES Separation of Duties	
NO DDoS Mitigation	NO Data Classification		
	YES IDS/IPS	NO Breach Notification	
Incident Detection and Response	YES Event Log Correlation and Analysis	YES Periodic Logical Access Revi	ew/Termination
incluent Detection and Response	YES Network Segmentation		
	YES Antimalware		
	YES Web application firewall	YES Third parties do not maintain	n access to dev/prod
Vendor Software/Application Security	YES Designated security personnel involved in SDLC	NO Production and developmen segmentation	t environment
	YES Security testing is part of build verification		
Password Policy For Employee Access	NO Multifactor authentication for administrative access		
Password Policy For Client Access	YES Multifactor authentication available for client access		



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.

IT Cloud Provider | Cloud Hosting System

Evendiligence[™]

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

Business Continuity		Regulation Mapping 🗹 LOW		
	Vendor has documented Business Continuity Plan (BCP)	Briefly describe documented process for service interruption or degradation		
	YES Vendor has documented Disaster Recovery Plan (DRP)	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		
Overview	NO Board of Directors or Senior Management provides oversight of the BCP	interruption. The plan is distributed and available to all necessary groups and is review upon hiring (for applicable		
	YES Plans undergo ongoing maintenance	roles) and re-reviewed and signed off on annually. The plan also includes notification parameters as appropriate.		
	YES Are employees trained on Business Continuity and Disaster Recovery			
	YES A Business Impact Analysis is performed	Frequency of testing Last tested Remediated		
	YES RTO Tested & Met	BCP Annually		
Business Continuity Plan Testing	Recovery Time Objective (RTO) and Comments >72 hours	DRP Annually 2/10/2023 5/3/2023		
business continuity i num resting	YES RPO Tested & Met	YES Distance between primary and alternate locations is appropriate		
	Recovery Point Objective (RPO) and Comments >24 hours	An alternative data center is available with the configuration of Warm		

Page 5/7

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.

IT Cloud Provider | Cloud Hosting System



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 Explana	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.				

Page 6/7

IT Cloud Provider | Cloud Hosting System



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**-**
SEC Regulation SCI reference to NIST 800-53 Rev. 4	800-53-**

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.