






# System and Organization Controls (SOC) Report Assessment

## Overall Vendor Risk Rating

<b>Service Provider, Inc. - Core System</b>	<b>Overall Rating</b>	Cautious: 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.
---	-----------------------	---

	<b>Reporting Period</b>	LOW		<b>Data Center</b>	MEDIUM
	<b>Organization and Administration</b>	LOW		<b>Control Objectives and Activities</b>	HIGH
	<b>Information System</b>	MEDIUM			

<b>Institution</b>	ABC Company
<b>Service Description</b>	The Vendor was noted as providing the following service(s) on behalf of the Client: Service Provider, Inc. - Core Processing
<b>Audit Firm</b>	Auditors, LLP
<b>Type</b>	SOC 1 Type II
<b>Report Period</b>	October 01, 2019 - September 30, 2020
<b>Gap Letter</b>	A bridge/gap letter was provided by management.
<b>Subservice Organizations</b>	<ul style="list-style-type: none"> <li>• Managed Security Service Provider</li> </ul>
<b>Assessment Date</b>	March 18, 2021

## SOC Report Assessment Preface

As part of our review on behalf of ABC Company ("Client"), Venminder, Inc. ("Venminder") reviewed documentation provided by Service Provider, Inc. ("Vendor"), created by Auditors, LLP ("Firm"). Firm examined Vendor's description and controls in-scope over the Core System system ("System"). In summary, based on their review, Firm agrees that the description of the System and its controls are suitably designed. Vendor attests that, in summary, its controls were suitably designed and operated effectively throughout the period, the description fairly represents the System, and the description does not omit or distort information relevant to the scope of the System.

## Venminder Assessment Review

In the opinion of Venminder, Client should Cautiously depend on the System based on the control environment documented within the report provided by Vendor. The SOC 1 Type II report identified several significant controls covering Administration, Risk Management, Software Development, Change Management, Access Control, Data Input, Physical Access, and Application Processing, each tested by Firm. Based on their review of Management's assertion, Firm noted a Qualified opinion for the provided report. Thus, it is the opinion of Venminder that Vendor poses a Moderate risk to the Client's overall information security.

The following in scope Information System control(s) had associated control activities listed within the report and were tested: Server Security, Logical Access Control, Separation of Duties, Change Management, Log Management, Backup Management, and Third-Party Assessments. The following in scope Information System control(s) were mentioned within the report but did not have any associated control activities tested: Principle of Least Privilege. Unmarked in scope control(s) were not mentioned or tested within the report. Without verification of untested in scope control(s), a risk rating of lower than Medium cannot be assessed to the Information Systems section.

The following in scope Data Center control(s) had associated control activities listed within the report and were tested: Electronic Access Control, Visitor Tracking, Security Guards, Uninterruptible Power Supply(ies), Fire Detection, Fire Suppression, Cooling and Conditioning, Camera System, and Temperature and Humidity Monitoring. The following in scope Data Center control(s) were mentioned within the report but did not have any associated control activities tested: Power System Maintenance. Unmarked in scope control(s) were not mentioned or tested within the report. Without verification of untested in scope control(s), a risk rating of lower than Medium cannot be assessed to the Data Center section.

Firm noted a Qualified Opinion, stating "The Description states that a formal user access certification process occurs semi-annually whereby managers re-authorize the appropriateness of access to systems and requests to remove access are completed systematically through the identity and access management tool or manually by system administrators in accordance with company policy. However, the control to remove the access as requested during the certification process was not suitably designed nor operating effectively throughout the review period. As a result, these controls were not suitably designed nor operating effectively to achieve the control objective."

Firm noted two (2) exceptions regarding the potential for unauthorized access and were rated as Medium risk. Based on these exceptions and the finding of a Qualified Opinion, a risk rating of lower than High cannot be assessed to the Control Objectives and Activities section.

### Recommendations:

Client is encouraged to request evidence that the controls identified by the auditor as not suitably designed nor operating effectively have been remediated and are performing as designed or that a remediation plan is in place.

Client is encouraged to request that Vendor demonstrates that the following unmentioned Organization and Administration controls are in place: Background Screening and Vendor Management.

Client is encouraged to request that Vendor demonstrates that the following untested Information Systems controls are in place: Network Security, Patch Management, Principle of Least Privilege and Incident Management.

Client is encouraged to request that Vendor demonstrates that the following untested Data Center controls are in place: Generators, Power System Maintenance, Fire System Maintenance, and Cooling and Conditioning System Maintenance.

## Subservice Organizations

### Services Provided by Vendor External Entities

The below is an overview of external entities of Vendor. Controls are not tested for these entities and are treated as out-of-scope for the audit performed. Client is responsible for the understanding of which subservice organizations apply to their contracted and utilized services. Subservice Organizations provide services, sometimes critical to operations, to Vendors undergoing review. Vendors do not always list Subservice Organizations within their SOC reports. Information available from the report in review is represented here.

### Vendor identified the following subservice organization(s):

- Managed Security Service Provider-Security operations center

## Reporting Period

LOW

A SOC reporting period can cover a period of time (Type II report) which covers controls that were in place and operating for a period of time, typically six to twelve months; or a point in time (Type I report); which audits controls as of a specific date by reviewing a single piece of evidence and includes a review of the suitability of those controls.

### Audit Date

October 01, 2019 through September 30, 2020

### Bridge/Gap Letter

A Bridge/Gap Letter for the period of September 30, 2020 through December 31, 2020 states that there have been no material changes to the control environment.



## Organization and Administration

LOW

### Summary of Vendor Representation

Vendor was founded in 2002 as a provider of core processing solutions for banks and credit unions. Vendor headquarters are in Elizabethtown, Kentucky and Des Moines, Iowa. Vendor also maintains a secondary support center in Denver, Colorado. Vendor's production systems rotate between data center facilities in Louisville, Kentucky and Des Moines, Iowa. Both facilities are owned and operated by Vendor. Executive and senior management structure is outlined and structured in a hierarchical manner. In addition to the controls below, Vendor noted that formal job descriptions are maintained, privacy training occurs during on-boarding, education verification occurs prior to hiring, and internal audits occur regularly. Vendor states they have a documented process to assess and manage risks associated with vendors and business partners.

The following Organization and Administration controls are documented within the provided SOC report:

- Board of Directors Involvement
- Background Screening
- Security Training
- Policy Acknowledgement
- Vendor Management



## Products and Services Summary

### Summary of Vendor Representation

Vendor provides its core system product to clients. The system includes both business and consumer interfaces. These products provide the client the ability to offer the ability for end- users to open accounts, look up loan and deposit account balances, look up account histories, transfer funds, originate Automated Clearing House (ACH) wire transactions, and make loan payments.



## Information System

MEDIUM

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Server Security              | <input checked="" type="checkbox"/> Change Management       |
| <input type="checkbox"/> Network Security                        | <input type="checkbox"/> Incident Management                |
| <input checked="" type="checkbox"/> Logical Access Control       | <input checked="" type="checkbox"/> Log Management          |
| <input type="checkbox"/> Patch Management                        | <input checked="" type="checkbox"/> Backup Management       |
| <input checked="" type="checkbox"/> Separation of Duties         | <input checked="" type="checkbox"/> Third Party Assessments |
| <input checked="" type="checkbox"/> Principle of Least Privilege |   |

### Venminder Review

The following in scope Information System control(s) had associated control activities listed within the report and were tested: Server Security, Logical Access Control, Separation of Duties, Change Management, Log Management, Backup Management, and Third-Party Assessments. The following in scope Information System control(s) were mentioned within the report but did not have any associated control activities tested: Principle of Least Privilege. Unmarked in scope control(s) were not mentioned or tested within the report. Without Verification of untested in scope control(s), a risk rating of lower than Medium cannot be assessed to the Information System section.

## Data Center Overview

**MEDIUM**

Venminder noted the following marked controls as in-place within Vendor's data center facilities.

Louisville, KY

Des Moines, IA

### Access Controls

The following access controls were covered within the scope of this report:

- Electronic Access Control
- Visitor Tracking
- Security Guards

### Environmental

The following environmental controls were covered within the scope of this report:

- |   |  |
|---|--|
| <input type="checkbox"/> Generator(s)                                 | <input checked="" type="checkbox"/> Cooling and Conditioning         |
| <input checked="" type="checkbox"/> Uninterruptible Power Supply(ies) | <input checked="" type="checkbox"/> Power System Maintenance         |
| <input checked="" type="checkbox"/> Fire Detection                    | <input type="checkbox"/> Cooling and Conditioning System Maintenance |
| <input checked="" type="checkbox"/> Fire Suppression                  | <input type="checkbox"/> Fire System Maintenance                     |

### Monitoring

The following monitoring controls were covered within the scope of this report:

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Camera System | <input checked="" type="checkbox"/> Temperature and Humidity |
|---|--|

### Venminder Review

The following in scope Data Center control(s) had associated control activities listed within the report and were tested: Electronic Access Control, Visitor Tracking, Security Guards, Uninterruptible Power Supply(ies), Fire Detection, Fire Suppression, Cooling and Conditioning, Camera System, and Temperature and Humidity Monitoring. The following in scope Data Center control(s) were mentioned within the report but did not have any associated control activities tested: Power System Maintenance. Unmarked in scope control(s) were not mentioned or tested within the report. Without Verification of untested in scope control(s), a risk rating of lower than Medium cannot be assessed to the Data Center section.

## 1 2 3 Control Objectives and Activities

HIGH

### Control Structure

Vendor organized their control structure to include Control Objectives from the following categories:

Administration, Risk Management, Software Development, Change Management, Access Control, Data Input, Physical Access, and Application Processing

### Control Coverage

The stated control objectives appear to be reasonable based on the nature of the services provided within the scope of this report. Exception risk ratings are for residual risk, accounting for management's response, if one was provided.

### Exceptions Noted

#### Exception 1

Control 5.9 and 6.2 - page 104 and 119

**Control Activity:** A manager completes a termination checklist to track the removal of access to the network for terminated employees.

**Testing Performed:** Inspected core application access listings for a sample of terminated users to determine whether their access was disabled or removed.

**Results of Testing:** 7 of 25 selected terminated employees access was not removed from the core application after user termination.

**Management Response:** none provided

*Impact -* Potential for unauthorized access

*Risk Rating -* Medium

## ⚡ Business Continuity and Disaster Recovery Planning

### Summary of Vendor Representation

Information regarding Business Continuity and Disaster Recovery Planning was not included in the provided report.

### 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



Sara B. Sample, CRVPM, CISSP  
Senior Information Security Specialist  
Venminder, Inc.

## Documentation Utilized

---

- Service Provider SOC 1 Type II Report.pdf
- 2019 Bridge Letter - Service Provider SOC 1 Type II.pdf

## Complementary User Entity Controls

---

The report indicates that certain control objectives specified in the SOC report can only be achieved if your organization is in compliance with the complementary user entity controls listed in the 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 following table summarizes the complementary user entity controls as stated in the SOC report.

Control	Responsibility	ABC Company Response
CC 1.1 User organizations are responsible for controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy.		
CC 1.11 and CC 1.2 User organizations are responsible for controls to ensure the confidentiality of any user IDs and passwords assigned.		
CC 6.2 and CC 6.3 User organizations are responsible for controls to immediately notify the Company of any actual or suspected information security breaches, including compromised user accounts.		

## Rating Explanations

---

Rating	Explanation
<b>LOW</b>	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.
<b>MEDIUM</b>	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.
<b>HIGH</b>	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.
<b>SEVERE</b>	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.