A-LIGN

People Center Inc. DBA Rippling

Type 2 SOC 3

2023

RIPPLING

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2022 to June 30, 2023

Table of Contents

SECTION 1

ASSERTION OF PEOPLE CENTER INC. DBA RIPPLING MANAGEMENT

ASSERTION OF PEOPLE CENTER INC. DBA RIPPLING MANAGEMENT

September 5, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within People Center Inc. DBA Rippling's ('Rippling' or 'the Company') Rippling Platform Services System throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Rippling's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "People Center Inc. DBA Rippling's Description of Its Rippling Platform Services System throughout the period July 1, 2022 to June 30, 2023" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Rippling's service commitments and system requirements were achieved based on the trust services criteria. Rippling's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "People Center Inc. DBA Rippling's Description of Its Rippling Platform Services System throughout the period July 1, 2022 to June 30, 2023".

Rippling uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Rippling, to achieve Rippling's service commitments and system requirements based on the applicable trust services criteria. The description presents Rippling's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Rippling's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Rippling's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Rippling's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that Rippling's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Rippling's controls operated effectively throughout that period.

Adam Nunn

Adam Nunn
Senior Director, Trust & Security
People Center Inc. DBA Rippling

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To People Center Inc. DBA Rippling:

Scope

We have examined Rippling's accompanying assertion titled "Assertion of People Center Inc. DBA Rippling Management" (assertion) that the controls within Rippling's Rippling Platform Services System were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Rippling's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Rippling uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Rippling, to achieve Rippling's service commitments and system requirements based on the applicable trust services criteria. The description presents Rippling's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Rippling's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Rippling, to achieve Rippling's service commitments and system requirements based on the applicable trust services criteria. The description presents Rippling's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Rippling's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Rippling is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Rippling's service commitments and system requirements were achieved. Rippling has also provided the accompanying assertion (Rippling assertion) about the effectiveness of controls within the system. When preparing its assertion, Rippling is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Rippling's Rippling Platform Services System were suitably designed and operating effectively throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Rippling's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Rippling's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Rippling's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Rippling, user entities of Rippling's Rippling Platform Services System during some or all of the period July 1, 2022 to June 30, 2023, business partners of Rippling subject to risks arising from interactions with the Rippling Platform Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
September 5, 2023

SECTION 3

PEOPLE CENTER INC. DBA RIPPLING’S DESCRIPTION OF ITS RIPPLING PLATFORM
SERVICES SYSTEM THROUGHOUT THE PERIOD
JULY 1, 2022 TO JUNE 30, 2023

OVERVIEW OF OPERATIONS

Company Background

Rippling gives businesses one place to run HR, IT, and Finance. It brings together all of the workforce systems that are normally scattered across a company, like payroll, expenses, benefits, and computers. For the first time ever, you can manage and automate every part of the employee lifecycle in a single system.

Based in San Francisco, CA, Rippling has raised $1.2B from the world’s top investors-including Kleiner Perkins, Founders Fund, Sequoia, Greenoaks and Bedrock.

For more information, visit Rippling.com.

Description of Services Provided

Rippling provides businesses around the world with solutions for both HR and IT. The company’s core service is a directory of employee information. This directory serves as the common data layer for all other Rippling services.

Primary services the company provides:

- Rippling Unity: unified workforce management platform
- HR Cloud: payroll, time and attendance, learning management, benefits, talent management, benefit administration
- IT Cloud: app management (single sign on, password management, multi-factor authentication, app provisioning) and device management (setup, security, ordering, shipping and storage, device offboarding)

Principal Service Commitments and System Requirements

Rippling has designed its processes and technology to serve the needs of its customers. Those needs include securing customer data and providing reliable access to the services a customer has subscribed to. Across the company, there are standards that are enforced in every service such as the encryption of data in motion and at rest, operating under the least privilege access model, and logging of events. In specific areas, processes have been implemented to address unique needs such as the documentation of sub processes for General Data Protection Regulation (GDPR) or encrypted e-mail for legacy partners.

Components of the System

Infrastructure

Primary infrastructure used to provide Rippling Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS	Cloud	Compute, networking, storage
MongoDB Atlas	Cloud	Storage

People

Rippling employees are grouped into the following organizations:

- Sales: The go-to-market teams at Rippling are centralized within the Sales organization. This includes all sales personnel, lead generation, and implementation

- Operations: This organization is led by the Chief Operating Officer (COO). It is both cross-functional and vertical. It is cross-functional in that the Operations team coordinates management activities across the entire company (metrics reporting, manager training, company-wide activities, facilities management, etc.) There are also two vertical teams that are embedded within the Operations organization, Design and Support, as these teams provide services to the entire company and the customer base
- Customer Experience: This organization is led by the Vice President of Customer Experience, and includes both the Customer Success and Customer Support teams who are responsible for delivering and ensuring an excellent experience for customers
- Product and Engineering: Product managers and software engineers are responsible for building and maintaining Rippling's services. The organization is run using a pod structure. Essentially each service is associated with a pod of product managers and engineers, supporting personnel, and a manager. These managers report to the Vice President of Engineering
- Security: This organization is led by the Chief Information Security Officer (CISO). Security is responsible for ensuring product security as well as monitoring the environment for continued security
- Marketing: Marketing at Rippling is responsible for lead generation, company brand, and external company communications
- Executive: The executive team at Rippling includes senior leadership across the company and is led by the company's Chief Executive Officer (CEO)
- Finance, Risk, and Data Analytics: Rippling's Finance team, led by the Chief Financial Officer (CFO), is responsible for all accounting and finance operations, risk, and data analytics at Rippling. This includes, but is not limited to, managing accounts payable, accounts receivable, financial reporting, strategic planning, budgeting, and variance analysis
- Legal and Compliance: The Legal and Compliance function, led by the General Counsel (GC), safeguards the business through the provision of legal advice and compliance infrastructure to ensure adherence to internal policies and law

Data

Please note: Rippling's customers may subscribe to services individually - as such, not every dataset applies to every customer.

Rippling's data includes the following Customer information:

- Employee data:
  - Demographics
  - Employment details
  - Benefit details
  - Bank details
- Company information:
  - Business details
  - Bank details
  - Hardware details
  - Service provider details

All users interact with this data through either a web browser or a native mobile application. All data is encrypted in motion and at rest. Role-based permissions are used to define customer access to various data sets they wish to share internally.

Data is exchanged between systems in a variety of ways. Rippling's preferred method of data exchange is an application programming interface (API) between systems. For single sign-on (SSO) interactions, the exchange may take place using an API or Security Assertion Markup Language (SAML). Finally, some of Rippling's health insurance partners prefer to exchange information using e-mail or fax. In these situations, Rippling personnel take appropriate measures to ensure that protected health information (PHI) is protected using encryption whenever possible.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Rippling policies and procedures that define how services should be delivered. These are located on the Company's shared drive and can be accessed by any Rippling team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system. Refer to the "Subservice Organizations" section below for controls managed by AWS.

Logical Access

Rippling software is used to manage access to applications, and access changes on role transitions and termination. Each application integrated with Rippling has a person or persons designated as the application admin. The application admin is responsible for configuring rules for application access, which include which departments, work locations, and employment types should get access to the application.

Additionally, application admins in Rippling perform reviews of application access quarterly, by verifying the application access rules and users on the Overview, Groups, and Matches tabs within each application on Rippling. Application admins must record that they've completed access reviews in a ticketing system.

Two-factor authentication is enabled, and enforced by policy, for accessing the Rippling site, SSO to other applications, and AWS Systems Manager to Secure Shell (SSH) production servers. Short message service (SMS) messages are not allowed as a valid two-factor authentication mechanism.

RPass is used for managing passwords for all third-party sites that don't support SAML links on the Rippling site.

Computer Operations - Backups

Rippling's fully-redundant production database is hosted in a SOC 2 compliant datacenter. The database is replicated across several availability zones in a multi-shared cluster topology. Moreover, continuous backups take incremental backups of data in the production database, ensuring backups are just a few seconds behind the operational system.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Rippling monitors the capacity utilization of its cloud computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Rippling leverages auto-scaling infrastructure that adapts its capacity in response to growth of existing customers and/or the addition of new customers.

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the environmental security controls for the in-scope system. Refer to the "Subservice Organizations" section below for controls managed by AWS.

Change Control

Rippling maintains documented systems development life cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. Additionally, file integrity monitoring (FIM) software is utilized to help detect unauthorized changes within the production environment.

Data Communications

Both traditional and web application-based firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Administrative access to the firewall is restricted to authorized employees.

High availability is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, load balancers, servers, and databases. In the event that a system fails, the redundant hardware is configured to take its place and launch Rippling services in a new healthy system.

Continuous penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Rippling. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

Vulnerability scanning is performed on a quarterly basis in accordance with Rippling policy. Rippling uses industry standard scanning technologies. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Additionally, an intrusion prevention system is utilized to analyze production environment events and report possible or actual production environment security breaches.

Rippling’s commitment to application security includes the continuous operation of a bug bounty program. Vulnerabilities found by security researchers are continuously monitored, triaged, and resolved by the security team, which elevates the overall security of Rippling’s application.

Authorized employees may access the system from the Internet through the use of leading agent-based out-of-band access. Employees are authenticated through Single Sign on protocol and the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Rippling Platform Services System performed at the San Francisco, California, New York, New York, and Seattle, Washington facilities.

This report does not include the cloud hosting services provided by AWS at multiple locations.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization’s last review.

Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System

All Common/Security, Availability, and Confidentiality criterion were applicable to the Rippling Platform Services System:

Requirements Not applicable to the System		
Safeguard	**Requirement**	**Reason**
Administrative Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
Physical Safeguard	164.310(c)	The entity is not a covered entity.
Organizational Safeguards	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1), 164.314(b)(2)	The entity is not a plan sponsor.
Breach Notification	164.404(a)(1), 164.404(a)(2), 164.404(b), 164.404(c)(1), 164.404(c)(2), 164.404(d)(1)(i), 164.404(d)(1)(ii), 164.404(d)(2), 164.404(d)(2)(i), 164.404(d)(2)(ii), 164.404(d)(3), 164.406, 164.408(a), 164.408(b), 164.408(c)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple locations.

Subservice Description of Services

AWS provides a suite of cloud hosting services, including data and application hosting, as well as automated backup services to customers internationally.

Complementary Subservice Organization Controls

Rippling's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Rippling's services to be solely achieved by Rippling control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Rippling.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria and HIPAA/HITECH requirements are met:

Subservice Organization - AWS		
Category / Safeguard	**Criteria / Requirement**	**Control**
Common Criteria / Security, Physical Safeguards	CC6.4, 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv)	Physical access systems are in place to restrict access to the facility and production equipment.
		Administrative access to the physical access systems is restricted to authorized personnel.
		Physical access to data centers is approved by an authorized individual.
		Physical access points to server locations are managed by electronic access control devices.
		Access to the facility is revoked as a component of the termination process or as requested by authorized personnel.
		A video surveillance system is in place to record access to the facility and is maintained for ad hoc review.
		Electronic IDSs are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.

Subservice Organization - AWS		
Category / Safeguard	**Criteria / Requirement**	**Control**
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs reviews of colocation service providers to validate adherence with AWS security and operational standards at least on an annual basis.
		S3-Specific - S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating, and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Rippling management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Rippling performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding discussions with vendors and subservice organization at least on an annual basis
- Reviewing attestation reports over services provided by vendors and subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Rippling’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Rippling’s services to be solely achieved by Rippling control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Rippling’s.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Rippling.
2. User entities are responsible for notifying Rippling of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Rippling services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Rippling services.
6. User entities are responsible for providing Rippling with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Rippling of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.