STRIVACITY®

STRIVACITY, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

STRIVACITY FUSION SERVICES SYSTEM

FOR THE PERIOD OF AUGUST 1, 2021, TO JULY 31, 2022

Attestation and Compliance Services

schellman
Quality, above all.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Strivacity, Inc.:

Scope

We have examined Strivacity, Inc.'s ("Strivacity") accompanying assertion titled "Assertion of Strivacity, Inc. Service Organization Management" ("assertion") that the controls within Strivacity's Strivacity Fusion Services system ("system") were effective throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that Strivacity'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Strivacity uses various subservice organizations for cloud hosting and managed detection and response services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Strivacity, to achieve Strivacity's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Strivacity 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 Strivacity's service commitments and system requirements were achieved. Strivacity has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Strivacity 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 whether 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 systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 controls were not effective to achieve Strivacity's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Strivacity's 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.
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 Strivacity's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 Strivacity's Strivacity Fusion Services system were effective throughout the period August 1, 2021, through July 31, 2022, to provide reasonable assurance that Strivacity's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Emphasis-of-Matter

Strivacity's description of its Strivacity Fusion Services system states that a ticketing system is utilized to document and evaluate incidents, responses, and resolution and that security and compliance personnel are alerted immediately when an incident involves unauthorized use or disclosure of personal information. However, during the period August 1, 2021, to July 31, 2022, no incidents occurred that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria: "CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.", "CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.", and "CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents." Our opinion is not modified with respect to this matter.

Schellman & Company, LLC

Columbus, Ohio
August 18, 2022

ASSERTION OF STRIVACITY SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Strivacity, Inc.'s ("Strivacity") Strivacity Fusion Services system ("system") throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that Strivacity's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 August 1, 2021, to July 31, 2022, to provide reasonable assurance that Strivacity'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Strivacity's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 August 1, 2021, to July 31, 2022, to provide reasonable assurance that Strivacity's service commitments and systems requirements were achieved based on the applicable trust services criteria.

Our description of our Strivacity Fusion Services system states that a ticketing system is utilized to document and evaluate incidents, responses, and resolution and that security and compliance personnel are alerted immediately when an incident involves unauthorized use or disclosure of personal information. However, during the period August 1, 2021, to July 31, 2022, no incidents occurred that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, the tests of operating effectiveness could not be performed for those controls as evaluated using trust services criteria: "CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.", "CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.", and "CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents."

DESCRIPTION OF THE BOUNDARIES OF THE STRIVACITY FUSION SERVICES SYSTEM

Company Background

Founded in 2019, Strivacity is a software company providing turn-key customer identity and access management (CIAM) solutions to brands selling their products and/or services in the digital marketplace. Strivacity's mission is to securely connect organizations to their customers while paving the way for lifetime relationships built on loyalty and trust. The Strivacity team is comprised of industry veterans with decades of security and identity experience, with offices in the United States and Europe. The Strivacity team members hold a shared belief that the basic tenets of security, privacy, and automation should not only help protect a business, but also drive it forward.

Description of Services Provided

Strivacity Fusion services provide simple and secure customer registration, adaptive multi-factor authentication, as well as privacy and consent management controls across all relevant digital channels. It provides customer and market insights and easily integrates with existing customer management and marketing solutions. Ready built components, well documented APIs, and easy to use software development kits (SDKs) built around customer-dedicated cloud services ensure quick time to value.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Strivacity Fusion Services system. Commitments are communicated in standardized contracts and service level agreements.

System requirements are specifications regarding how the Strivacity Fusion Services system should function to meet Strivacity's principal commitments to user entities. System requirements are specified in Strivacity's policies and procedures, which are available to all employees.

[Intentionally Blank]

Strivacity's principal service commitments and system requirements related to the Strivacity Fusion Services system include the following:

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Security	• System access is granted to authorized personnel only • Protection of data at rest and in transit • Regular security assessments • Identification, remediation, and customer notification of security incidents/events • Develop, implement, and maintain an information security program designed to protect the security, integrity, and confidentiality of the system and its information • Notification of any scheduled maintenance to customers at least 48 hours in advance of scheduled maintenance • Provide support services hours from Monday - Friday, 6AM - 6PM	• Logical access standards • Employee provisioning and deprovisioning standards • Access reviews • Risk and vulnerability management standards • Configuration management • Incident handling standards • Change management standards • Vendor management
Availability	• Ability to recover and restore customer data • 99.99% Monthly Uptime • Provide response times less than 1000 milliseconds for sustained period of 5 minutes for API • Provide response times less than 3000 milliseconds for sustained period of 5 minutes for any user interface	• System monitoring • Backup and recovery standards
Confidentiality	• Maintain all customer data as confidential and not to disclose information to any unauthorized parties without written consent • Protection of data at rest and in transit	• Data classification • Retention and destruction standards • Data handling standards

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Strivacity is hosted at Amazon's Web Services (AWS) via Kubernetes environments. It is micro service based, with containers running Ubuntu or Alpine Linux virtual machines.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Strivacity Fusion	Strivacity's CIAM platform providing adaptive access control, customer lifecycle management, marketing and insights, and global privacy and consent services.	AWS EC2 / Linux AWS RDS / Aurora MySQL	Multiple AWS Regions
	Utilized for storage of user data.	MongoDB	

People

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- IT and Engineering personnel – responsible for risk management and identification, monitoring, and compliance of security issues and incidents throughout the service delivery infrastructure.

Procedures

Access Authentication and Authorization

An acceptable use policy is in place to guide personnel in the acceptable and secure use of corporate assets. The in-scope systems are configured to authenticate users with an authorized user account, password, and token before granting access. An encrypted VPN is required for remote access to production and enforces multi-factor authentication. Passwords to service, application, shared and root accounts are centrally maintained in an encrypted vault restricted to authorized employees. Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems. Administrator access to the in-scope systems is restricted to user accounts accessible by authorized personnel. Virtual Private Cloud (VPC) security groups are in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that is not explicitly authorized by a rule.

Access Requests and Access Revocation

Employee access requests are documented and require the approval of management prior to access being granted. System access is revoked for employees as a component of the employee termination process. User access reviews, including privileged users, are performed by management on a monthly basis to ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.

Change Management

Documented policies and procedures are in place to guide personnel in the release management and change management process. A ticketing system is utilized to track and document changes throughout the change management process. Application and system changes are tested and must be approved by engineering and customer success leadership prior to implementation into production. The production environment is logically segmented from the development and test environments. Customer data is not utilized for application change control development or testing. The ability to implement application and system changes into the production environment is restricted to user accounts accessible by authorized personnel without development responsibilities. A change management meeting is held on a weekly basis to discuss high-risk changes that affect the system.

Data Backup and Disaster Recovery

A business continuity plan and a disaster recovery plan are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. Disaster recovery personnel perform an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system

requirements. Documented policies and procedures are in place to guide personnel in the data backup and restoration process. An automated backup system is in place and scheduled to perform backups on a daily basis. The automated backup system is configured to monitor the status of data backups and send an alert notification to operations personnel upon backup failure. Management performs data restoration as a normal component of business operations to help ensure the recoverability of customer production data.

Incident Response

An incident response plan for reporting security, availability, and confidentiality incidents is in place and provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints. A ticketing system is utilized to document and evaluate incidents, responses, and resolution. Security and compliance personnel are alerted immediately when an incident involves unauthorized use or disclosure of personal information. When an incident is identified, the security and compliance team will create an incident ticket within the ticketing system with the details of the event and assign the ticket a severity level. Upon the creation of the incident ticket, the incident response team immediately initiates an investigation to assess the scope and impact of the situation, and to determine the actions necessary for mitigation. Mitigation includes the prevention of any continued loss of data or services, valuation of existing controls, a forensic analysis of the event, and the required notifications of any regulatory and or impacted entities.

System Monitoring

Internal and external vulnerability assessments of the production environment are performed utilizing a third-party vulnerability scanner on a quarterly basis. Remediation plans are documented and monitored through resolution. VPC security groups are in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that is not explicitly authorized by a rule.

Data

The following table describes the information used and supported by the system:

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer data processed by the Fusion application	Reported via the administrative console.	Confidential
Multiple threat information data bases (GEO-IP, botnet, malicious activity)	No reporting. Purchased from a third-party.	
Application state database (ephemeral tokens used by customers)	Reported via the administrative console.	
Fusion application logs	Reported via the log aggregation system.	Restricted
VPN access logs for personnel accessing production environments	Reported via the administrative console.	
Breach password static database (hashed password check against known breaches) deployed with each customer environment	No reporting. Updated automatically for each customer environment.	Public

Subservice Organizations

The cloud hosting services provided by Amazon Web Services (AWS) and the managed detection and response services provided by Expel, Inc. (Expel) were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS and Expel, alone or

in combination with controls at Strivacity, and the types of controls expected to be implemented at AWS and Expel to meet those criteria.

Control Activities Expected to be Implemented by AWS and Expel	Applicable Trust Services Criteria
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Strivacity Fusion Services system resides.	CC6.1 – CC6.3, CC6.6
AWS is responsible for managing and controlling access to the encryption keys to storage devices for its cloud hosting services where the Strivacity Fusion Services system resides.	CC6.1, CC6.7
AWS is responsible for ensuring that physical access control systems are in place at the data center to protect production and backup systems, respectively, from physical threats.	CC6.4 – CC6.5
Expel is responsible for monitoring the in-scope systems for security vulnerabilities and breaches and alerting Strivacity operations personnel upon the detection of certain security events, unusual system activity, or service requests.	CC6.6, CC7.1 – CC7.2
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Strivacity Fusion Services system resides.	CC6.7
AWS is responsible for restricting physical access to backup media, identifying, and addressing environmental vulnerabilities, and changing environmental conditions through the use of environmental protections.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Strivacity Fusion Services system.