Symphony Communication Services, LLC
Symphony SaaS Platform

Report on the Design and Operating Effectiveness of Controls at Symphony Communication Services, LLC, relevant to the Security, Availability, and Confidentiality Trust Services Principles

SOC 3 Type II

July 1, 2020 – June 30, 2021

SECTION ONE

Independent Service Auditor’s Report

Deloitte & Touche LLP
500 College Road East
Princeton, NJ 08540-6635
USA
Tel: +1 973 602 6000
Fax: +1 212 602 5050
www.deloitte.com

Independent Service Auditor's Report

Symphony Communication Services, LLC
1 World Trade Center
New York, New York 10007

Scope

We have examined Symphony Communication Services, LLC's ("Symphony") accompanying assertion titled "Assertion of Symphony" (assertion) that the controls within Symphony's software-as-a-service platform (system) were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that Symphony'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 Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The description of the boundaries of the system indicates that certain applicable trust services criteria specified in the description of the boundaries of the system can be met only if complementary user-entity controls contemplated in the design of Symphony's controls are suitably designed and operating effectively, along with related controls at Symphony. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

As indicated in the description of the boundaries of the system, Symphony uses Amazon Web Services and Google Cloud Provider ("subservice organizations") for its cloud computing platform and application hosting services. The description of the boundaries of the system indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system presents the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain 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 extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period July 1, 2020 to June 30, 2021.

Service Organization's Responsibilities

Symphony 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 Symphony's service commitments and system requirements were achieved. Symphony has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Symphony is responsible for selecting, and identifying in its assertion, the applicable trust service 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 system 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 Symphony's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Symphony's service commitments and system requirements based 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 the service organization'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.

Emphasis of a Matter

Controls related to supporting that the entity disposes of confidential information at the end of a contract agreement upon customer request did not operate during the period July 1, 2020 to June 30, 2021 because there were no occurrences of customers requesting disposal of their information at termination of their contract agreement with Symphony during the examination period. Therefore, we could not test the operating effectiveness of controls related to Criteria C1.2, "The entity disposes of confidential information to meet the entity's objectives related to confidentiality".

Opinion

In our opinion, except for the matter giving rise to the modification, management's assertion that the controls within Symphony's software-as-a-service platform were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that Symphony's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte & Touche LLP

December 21, 2021

SECTION TWO

Symphony Communication Services, LLC
Management Assertion

Assertion of Symphony

We are responsible for designing, implementing, operating and maintaining effective controls over the information systems and technology supporting Symphony Communication Services, LLC's (the "Service Organization" or "Symphony") Secure Messaging system throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that Symphony's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A below and identifies the aspects of the system covered by our assertion.

Symphony uses Amazon Web Services ("Amazon") and Google Cloud Platform ("Google") (collectively "subservice organizations") for its cloud computing platform and application hosting services. The description of the boundaries of the system includes only controls and applicable trust services criteria of Symphony and excludes controls and applicable trust services criteria of Amazon and Google. The description of the boundaries of the system indicates that the applicable trust services criteria specified in the description can be achieved only if controls at the subservice organizations contemplated in the design of Symphony's controls are suitably designed and operating effectively, along with the related controls at Symphony. We have not evaluated the suitability of the design or operating effectiveness of such subservice organization controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Symphony'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. Symphony'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 Attachment B 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, except for the matter giving rise to the modification of the opinion, the controls within the system were effective throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that Symphony's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A – Symphony's Description of the Boundaries of its SaaS platform

Symphony offers a Software-as-a-Service (SaaS) platform providing secure message and content sharing for organizations. The Symphony application is hosted by third-party hosting service providers Amazon Web Services ("Amazon") and Google Cloud Platform ("Google"). Customers access Symphony through their web browser (e.g. Internet Explorer, Chrome, Safari), using an installed desktop wrapper, or mobile application.

Customer message content is stored encrypted on Symphony production servers in the customer's dedicated cloud instance ("pod"). To the extent a customer sends content to another customer over the Symphony platform, customer content will be transmitted to such other customer and stored on both customer pods. Encryption keys are stored in the customer's Security Module and required to decrypt message content.

The core components of the Symphony platform include the pod comprised of the Java application and MongoDB database installed on Unix servers hosted at Google and Amazon.

This report covers the Symphony SaaS platform, Symphony personnel access to the production environments at third-party hosting service providers Amazon and Google, and certain logical and physical security perimeter controls around the Symphony corporate network and offices.

Complementary Subservice Organization Controls (CSOC)

Symphony uses subservice organizations Amazon and Google to perform various functions to support the delivery of services. The scope of this report does not include the controls and related criteria for which Amazon and Google are responsible, including:

- Maintaining physical security over its data center in which the servers used to host the Symphony SaaS platform are housed.
- Maintaining environmental security over its data center in which the servers used to host the Symphony SaaS platform are housed.

Complementary User Entity Controls (CUEC)

User entities are responsible to have certain controls in place to support the delivery of services. The scope of this report does not include the controls and related criteria for which user entities are responsible, including:

- Granting and revoking Symphony access to their users as appropriate, for periodically reviewing such access to ascertain access remains appropriate, and for monitoring access logs and addressing discrepancies.
- Enforcing use of unique IDs and for configuring password parameters to Symphony, or

their directory service where a directory service sync is utilized, which authenticates users to Symphony in accordance with their internal policies.

- Restricting physical access to Symphony components, if the customer elects to maintain these on their premises (e.g. hardware security module).
- Implementing security measures to protect their network from external threats (e.g., firewalls).
- Securing content once it is exported from Symphony (e.g., content exported utilizing the Symphony Export Bridge).
- Implementing anti-virus software in their environment to prevent or detect and act upon the introduction of unauthorized or malicious software.
- Implementing additional layers of security over connectivity to their pod as deemed necessary (e.g. direct connection), for customers not utilizing Symphony's VPN or whitelisting offerings.
- Communicating updates to whitelisted IP addresses in a timely manner, for customers using Symphony's IP whitelisting services.

Attachment B

Principal Service Commitments and System Requirements

Symphony has implemented controls designed to meet the criteria applicable to the security, availability, and confidentiality trust service principles, which state that the system is protected against unauthorized access, use, or modification, is available for operation and use as committed or agreed, and information designated as confidential is protected as committed or agreed.

Security, availability, and confidentiality commitments regarding the system are documented and communicated in signed customer agreements. Such commitments include, but are not limited to, the following:

- Securing customer message content through end-to-end encryption to restrict access to authorized parties.

- Enforcing policies and standards for the protection and safe handling of confidential information.

- Achieving the service level metrics defined in the customer agreement through leveraging infrastructure from highly-available third-party hosting service providers and employing load balancing.

Symphony establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Symphony's policies and procedures and customer agreements, as follows:

- The Information Security Policy establishes the foundation of security principles, and the framework of standards, that apply to the development, acquisition, operation, maintenance, and securing of information systems used by Symphony.

- The Service Level Agreement within the Master Services Agreement defines the service levels Symphony will meet or exceed as a percentage of service availability.

- The Information Classification and Handling Standard establishes classifications of information and defines handling guidelines and requirements to protect information from unauthorized disclosure, modification, destruction, or disruption of access.