OneSpan

SOC 3®– SOC for Service Organizations:

Trust Services Criteria for General Use Report

Report on OneSpan's Assessment of Security, Confidentiality, Availability and Privacy Controls for its OneSpan Digital Agreements and Authentication Solutions System

For the period January 1, 2023 to December 31, 2023

TABLE OF CONTENTS

KPMG LLP
600 de Maisonneuve Blvd. West
Suite 1500, Tour KPMG
Montréal Québec H3A 0A3
Tel 514-840-2100
Fax 514-840-2187
www.kpmg.ca

INDEPENDENT SERVICE AUDITORS' REPORT

To: Management of OneSpan Inc.

Scope

We have been engaged to report on OneSpan Inc.'s (OneSpan's) accompanying statement titled "Statement by Management of OneSpan" (the Statement) that the controls within OneSpan's Digital Agreements and Authentication Solutions System (the System) were suitably designed and operating effectively throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

OneSpan uses the subservice organizations identified in management of OneSpan's Attachment C – OneSpan's Complementary Subservice Organization Controls (Attachment C). Management of OneSpan's Attachment C indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OneSpan, to achieve OneSpan's service commitments and system requirements based on the applicable trust services criteria. Management of OneSpan's Attachment C presents the types of complementary subservice organization controls assumed in the design of OneSpan's controls. Management of OneSpan's Attachment C does not disclose the actual controls at the subservice organizations. Our engagement 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

OneSpan 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 OneSpan's service commitments and system requirements were achieved. Management of OneSpan has provided the accompanying Statement about the suitability of the design and operating effectiveness of controls within the System. OneSpan is also responsible for preparing the Statement, including the completeness, accuracy and method of presentation of the Statement; providing the services covered by the Statement; selecting, and identifying in the Statement, the applicable trust service criteria; identifying the risks that threaten the achievement of OneSpan's service commitments and system requirements; and having a reasonable basis for the Statement by performing an assessment of the suitability of the design and operating effectiveness of the controls within the System.

Our Independence and Quality Management

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility, under this engagement, is to express an opinion, based on the evidence we have obtained, on whether the Statement, that controls within the System were suitably designed and operating effectively throughout the period to provide reasonable assurance that the OneSpan's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether the Statement 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 reasonable assurance engagement included:

- obtaining an understanding of the System and OneSpan's service commitments and system requirements;
- assessing the risks that controls were not suitably designed or did not operate effectively to achieve OneSpan'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 suitably designed to provide reasonable assurance that OneSpan would achieve its service commitments and system requirements based the applicable trust services criteria if those controls operated effectively;
- testing the operating effectiveness of controls within the System to provide reasonable assurance that OneSpan achieved its service commitments and system requirements based on the applicable trust services criteria; and
- 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 suitability of the design and operating effectiveness of controls is subject to the risk that controls may become ineffective because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, the Statement that the controls within OneSpan's Digital Agreements and Authentication Solutions System were suitably design and operating effectively throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Chartered Professional Accountants

Montreal, Quebec
July 5, 2024

STATEMENT BY ONESPAN MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within OneSpan Inc.'s (OneSpan's) Digital Agreements and Authentication Solutions System (the System) throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, availability and privacy (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 in our Attachment A – OneSpan's Overview of Services and the Digital Agreements and Authentication Solutions System (Attachment A) and identifies the aspects of the System covered by our Statement.

OneSpan uses the subservice organizations identified in our Attachment C – OneSpan's Complementary Subservice Organization Controls (Attachment C). Our Attachment C indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OneSpan, to achieve OneSpan's service commitments and system requirements based on the applicable trust services criteria. Our Attachment C presents the types of complementary subservice organization controls assumed in the design of OneSpan's controls.

We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the applicable trust services criteria. OneSpan'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 our Attachment B – OneSpan's Principal Service Commitments and System Requirements (Attachment B).

We confirm that the controls within the System were suitably designed and operating effectively throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that OneSpan' service commitments and system requirements were achieved based on the applicable trust services criteria.

E-SIGNED by Steve Dukas
on 2024-07-05 13:01:45 EDT

Steve Dukas - Chief Information Security Officer
July 5, 2024

ATTACHMENT A – ONESPAN'S OVERVIEW OF SERVICES AND THE DIGITAL AGREEMENTS AND AUTHENTICATION SOLUTIONS SYSTEM

OneSpan Digital Agreements and Authentication Solutions Description

The OneSpan Transaction Cloud Platform is composed of the following solutions (the "Services"):

- OneSpan Sign (OSS), including the optional Virtual Room feature;
- OneSpan Notary (Notary);
- Identity Verification (IDV);
- Intelligent Adaptive Authentication (IAA); and
- OneSpan Cloud Authentication (OCA).

OneSpan Sign (OSS)

OneSpan Sign is an e-signature solution that enables users to prepare, send and sign documents over the web electronically. This process typically requires five steps:

- Upload documents for the signature process;
- Add recipients who will either be signing or reviewing the documents;
- Define who will be signing and where the signatures will need to be applied;
- Select the authentication method (username/password, secret question/answer, one-time passcode (OTP), third-party authentication services); and
- Initiate signature process.

An email is sent to each signer, inviting them to e-sign the document(s). If Users are face-to-face with the signer, they can use their computer or mobile device to capture the signer's signature. Each signer is guided step-by-step through the signing process. Once the documents are signed, they can be downloaded. The e-signed documents can then be downloaded for retention in the User's record system and deleted from OneSpan Sign. The e-signed documents are standard PDF files that can be viewed in Adobe Reader and other PDF readers.

Organizations use OneSpan Sign in three ways:

- Standalone web-based service (Professional Plan): This option is for the most common signing workflows and e-contracting use cases – for example, getting contracts and agreements electronically signed. Users upload a document, select their signers and begin e-signing;

- Integration (Enterprise Plan): Our solution gives users the ability to add e-signing capabilities into their own applications – whether that's through their website, mobile app, or even their home-grown or legacy system. We have an open, industry-standard REST API and fully supported SDKs for Java, .NET, APEX, iOS and Android – to help users embed e-signing capabilities in ANY one of their applications; and
- Using pre-built connectors for 3rd party applications.

OneSpan Sign E-Signature Workflow

Users create and send out digital documents and e-forms to clients for signing. OneSpan Sign manages the online signing process so that electronically signed contracts and records are enforceable, compliant and secure. In addition, customers can monitor all in-progress transactions, identify issues and take action to keep digital processes moving forward. See Figure 1 below for a typical e-signature transaction workflow.

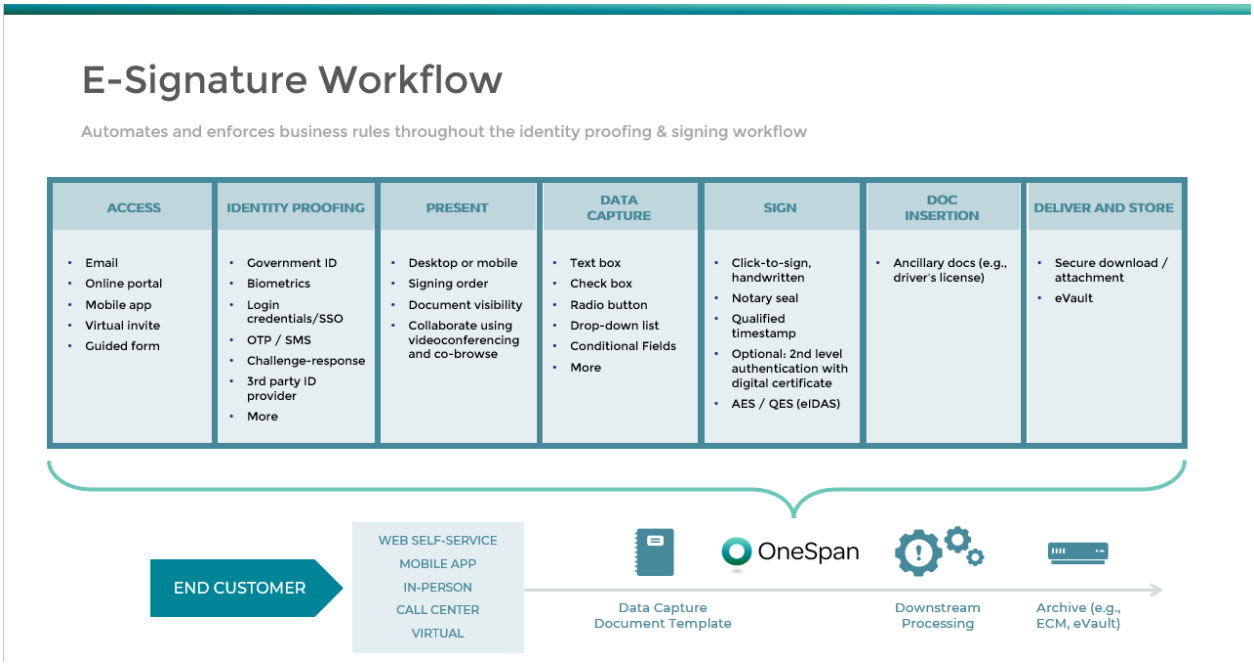

Figure 1: E-signature transaction workflow with OneSpan Sign

Customers can authenticate using various methods, including email, ID Verification, SMS, Question and Answer, and third-party authentication services. Digital encryption securely seals each signature block after signing, and the embedded audit trail reports on who signed, in what order, at what time and in what locations. This audit trail travels with the e-signed document and can be verified with one simple click to help ensure the document's integrity.

Virtual Room

OneSpan Virtual Room brings together electronic signature, web-enabled videoconferencing, and collaboration capabilities in one solution, including the following features:

- Captures, admissible, and enforceable e-signatures in near real-time;
- Built-in videoconferencing with signers in different locations;
- Verification of identities of the participants in the virtual signing session;
- Co-browsing feature to simultaneously review documents with signers and address their questions in near real-time; and
- Vendor-independent audit trails with the option to record the virtual signing session.

End-User Access to the System

Users can access the System via its secure web interface using their unique username (email address) and password. Integrated customers can also access the service through its Application Programming Interface (API) using an API key. All connections are made over HTTPS (TLS 1.3 by default) using secure ciphers, such as AES-256.

OneSpan Notary

The OneSpan Notary is a SaaS service that enables commissioned Notaries employed by business entities to perform In-Person Electronic Notarizations and Remote Online Notarizations. OneSpan Notary includes the following (as further defined in the OneSpan Notary Documentation) as part of the subscription fee (some features may not be used in an IPEN session due to the nature of an IPEN):

- Web-based e-signing process that provides options for the presentation and review of documents, methods of signature capture and user authentication, data capture and form fields;
- Workflows, reminders and notifications, attachments, and e-delivery of the Documents to Participants;
- OneSpan Sign Transaction management features for preparing and sending Documents manually through the user interface or using OneSpan Sign Transaction templates, and the ability to monitor and manage Documents that are in progress or completed;
- Electronically signed Documents in PDF format with each e-signature digitally signed for comprehensive security and detection of any Document changes along with an embedded audit trail;
- An Evidence Summary Report is provided for the e-signature experience and both the electronic evidence and summary are protected by digital signing;

- Recorded Notary Transaction capabilities that combine e-signature, video-conferencing, co-browsing, and recording capabilities into a single solution;
- Identity verification capabilities that incorporate the components necessary to facilitate the automated verification of a Participant's identity; and
- Notarization capabilities including, but not limited to, Notary onboarding, the Notarial Journal, digital certificates, ability to upload notarial seal, and Participant authentication.

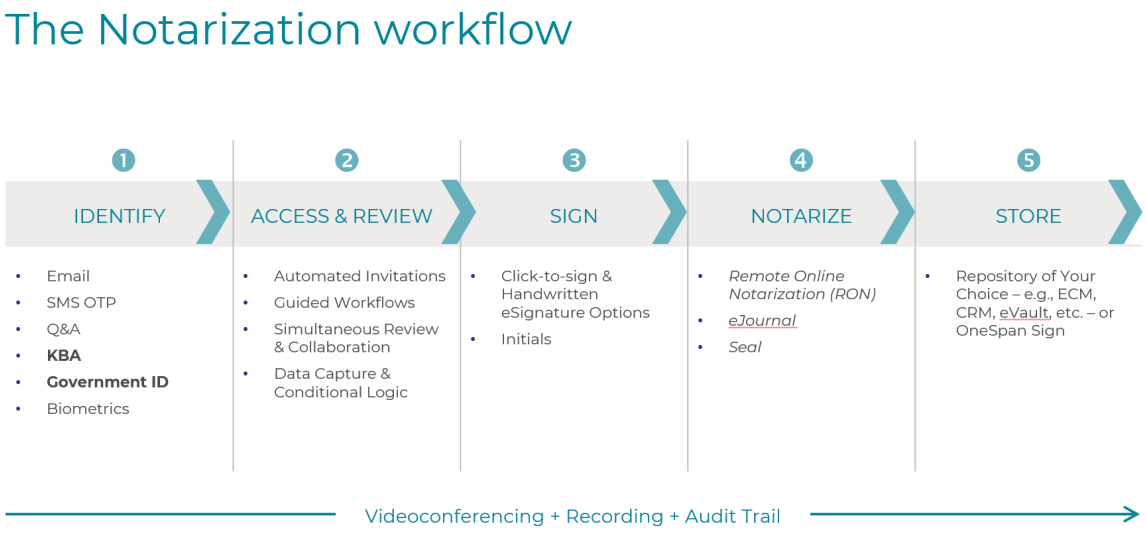

Figure 2: The notarization transaction workflow

Identity Verification (IDV)

OneSpan Identity Verification (IDV) digitizes the customer journey for digital identity verification while capturing and managing all supporting evidence. IDV is comprised of the following modules:

- Workflow Management;
- Identity Verification Hub; and
- Audit Trail Capture and Management.

The solution provides the following functionality:

- Digital identity verification validates the authenticity of an identity document (e.g., passport, identity card, driver's license). It checks whether the person presenting the identity document is the genuine owner of the document via facial comparison;
- Secure document signing, which digitally signs documents for account opening and financial transactions; and
- Digital audit trails of the entire agreement process, including identification checks and all actions performed by the customer. This includes recording all web pages presented to the customer during the agreement process. Supports web page replay with an event timeline to reveal what the customer did and saw during the agreement process.

Intelligent Adaptive Authentication (IAA)

The Intelligent Adaptive Authentication (IAA) solution secures web applications of customers by providing integration of authentication functionality into these web applications.

The authentication functionality secures logins into web applications and transactions, or payments initiated from the web applications. The solution assesses which authentication or transaction security measures are appropriate for each unique end-user at any given moment, taking into account the characteristics of the user or transaction as well as the user's behaviour and devices. Customers are typically financial institutions that want to protect access to their online banking applications and ensure a smooth, frictionless authentication experience for their end-users.

OneSpan Cloud Authentication (OCA)

The OneSpan Cloud Authentication (OCA) solution secures web applications of customers by providing easy integration of authentication functionality into these web applications. The authentication functionality secures logins of end-users into web applications as well as transactions initiated by end-users from the web applications.

In the context of this solution, customers are financial institutions or enterprises that wish to protect access to their web applications.

Components of the System Providing the Services

This section describes infrastructure, software, people, procedures, data, and privacy practices used to deliver the Services.

Infrastructure

By leveraging cloud partners, the OneSpan Digital Agreements and Authentication Solutions System can scale the required infrastructure resources whenever the need arises. OneSpan's cloud partners have extensive global data center networks. This provides OneSpan with an environment that is highly available with a disaster recovery capability to another geographic region.

OneSpan regularly reviews its cloud partners' compliance to validate that controls in place are sufficient to meet OneSpan's requirements.

The infrastructure is split into multiple network segments and firewall technology is used to control network traffic and allow required traffic. System instances are hardened to help ensure that required services are running. Administrative access to the system requires multifactor authentication. User accesses are logged and controlled, and mechanisms are in place to help prevent system abuse.

The Digital Agreements and Authentication Solutions System is monitored on a 24/7 basis, including through the use of intrusion detection tools. Events are centrally correlated, providing system administrators with continuous visibility over, and automated notifications in case of potential incidents, including system health or security.

Vulnerability scanning and intrusion tests are performed periodically through the use of tools to detect areas that require patching or other remediation to help protect against outside threats. Patches are applied regularly to help ensure the system stays up to date and secure.

Software

The system is designed based on a 3-tier architecture approach, comprised of different types of instances. Unless otherwise indicated, customer instances are built from standardized Images and are hardened as per OneSpan's hardening guidelines.

- **Presentation layer**: This layer is running public-facing instances in the form of load balancers, outbound proxies, and microservices to allow secure inbound traffic to the system and outbound traffic to integrated customers and interfaces to external third-party services.
- **Application layer**: This layer controls the Digital Agreements and Authentication Solutions System's functionalities. It hosts the system's front-end web services and back-end instances handling all the business logic associated with the Services, including the API requests.
- **Database layer**: Database instances supporting the system are running in this layer. Databases reside on encrypted volumes for data protection. Backups and replication of the data are performed in multiple zones and datacenters for high availability and disaster recovery purposes.

People

Multiple roles are defined, along with their responsibilities, such as Chief Information Security Officer, Data Protection Officer, Cloud Operations Director, Change Manager, Human Resources Manager, Product Management team, System Owner, Product Owner, Release Manager, R&D team, Senior Developers, Product Security team.

Our customers are user entities of the system who are OneSpan's direct customers or clients, such as a bank, with whom we have established service agreements to use our services and system. The end users of the system include our customers' customers who interact with the system. The system collects, processes, stores, and reports both confidential customer data and end-user data including personal information. From a privacy perspective, OneSpan acts as a data processor on behalf of its customers.

Procedures

OneSpan has developed procedures and processes to restrict logical access to the system and protect customer data. These procedures and processes are communicated to employees, and reviewed and updated as required to maintain system security. They cover multiple aspects, such as risk management, access controls, secure development, system hardening, change management, patch management, vulnerability management, business continuity, disaster recovery, and incident response.

Data

OneSpan Sign

The data captured by the system is as follows:

- Signer information;
- Signature information; and
- Documents requiring signatures.

The system captures and stores data necessary to carry out the electronic signing of documents. All of this data is coming through to the system via its REST API. Both integrated customers and the system's own web User Interface interact with this API over secured HTTPS connections.

The typical data creation workflow is the following: a user creates a document package, which represents the business transaction that needs signatures for completion. That document package contains metadata about the business transaction, including all of the Signer contact information, the documents that need to be signed or accepted and the signature location and format. The documents that are uploaded to the System are rendered into the PNG image format in order to present them in web browsers. These PNG images are also saved in the system database. Once the document package is ready to be signed, Signers are invited via email to sign the documents over the web.

When the Signers sign the documents, the documents get digitally signed using security certificates. These signed documents are then stored in the system database and made available for download to the Signers. Key information that is saved as part of the evidence and audit trail of the signing process is as follows:

- Date and time of signing;
- Signer's IP address;
- Documents and pages viewed by the Signer; and
- Values (if any) entered in document fields by Signers.

At the end of the signing process, Signers and or integrated customer systems can download the signed documents. They can also download the field values (if any) that were entered by Signers at the time of signing. This is called the “Evidence Summary,” which, as its name indicates, is a summary of the audit trail accumulated during the signing process and presented as a PDF document, which can also be downloaded.

While all of the previous data descriptions apply to the data related to the electronic signing of documents, the system also maintains information about its users. Basic account and user details are saved in the system database to allow users to access the system. The account can be created in a self-served fashion or by the Customer Support team. From then on, the newly created Customer Account Administrator can invite additional users to the system. User profile information can be edited by Users directly using the system interface.

In order to get visibility over the use of the System by Users, Customer Account Administrators can export system usage reports in the form of comma-separated value (CSV) files.

Intelligent Adaptive Authentication (IAA)

Data is collected for performing strong authentication of end-users for access to the client's application and for fraud risk analysis of transactions.

Not all customers provide the same data. Collected data may consist of:

- Card payment details;
- Credit card information;
- End-user DIGIPASS serial number;
- End-user personal information; and
- Technical information.

OneSpan Cloud Authentication (OCA)

Data is collected for performing strong authentication of end-users for access to the client's web application. Collected data may consist of name, phone, email, push notification ID, IP address, and DIGIPASS Serial Number.

Identity Verification (IDV)

Processing of personal data is done on behalf of the client to conclude agreements (e.g., end-to-end loans, consumer credit applications), perform identity verification, and facilitate contract execution and downstream processing (e.g., returning agreements to data subjects and retention for a limited period of time). Collected data may consist of name, address, phone, email, IP, sex, race, age, contact details, geographical data, facial picture, and banking details.

ATTACHMENT B – ONESPAN'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Service Commitments

OneSpan designs its processes and procedures related to its Digital Agreements and Authentication Solutions System to meet its objectives. Those objectives are based on the service commitments that OneSpan makes to its user entities, applicable laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that OneSpan has established for the Service.

Service commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, such as the OneSpan Terms and Conditions, which are published online (onespan.com). Service commitments include the following:

Security:

OneSpan's security objective for the system is to maintain and operate security controls such as multi-factor authentication, encryption and other relevant security controls to help support the protection of customer data and personal information from unauthorized access, disclosure, modification, or loss.

Availability:

OneSpan has made commitments related to percentage uptime and connectivity for the system, as well as commitments related to service credits for instances of downtime as defined in the service terms.

Confidentiality:

OneSpan has made commitments related to designing and implementing controls to help support the confidentiality of customers' data through data classification policy, data encryption and other relevant security controls.

Privacy:

OneSpan has made commitments related to designing and implementing controls to help support the protection of personal information and complying with applicable privacy laws and regulations. For clients, OneSpan acts as the data processor.

System Requirements

OneSpan has established operational requirements that support the achievement of service commitments, compliance with applicable laws and regulations, and other system requirements. Such requirements are communicated in OneSpan's policies and procedures, system design documentation, and contractual agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the system is designed, developed, and operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system.

ATTACHMENT C – ONESPAN'S COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

OneSpan's Digital Agreements and Authentication solutions were designed with the assumption that certain control objectives can be achieved only if complementary subservice organization controls assumed in the design of OneSpan's controls are suitably designed and operating effectively at the identified subservice organizations, along with the related controls at OneSpan.

OneSpan uses the infrastructure services of AWS to host OneSpan's Digital Agreements and Authentication solutions and to support the achievement of the control objectives identified in this report. The subservice organization controls presented below should not be regarded as a comprehensive list of all of the controls that should be employed by the subservice organizations.

SUBSERVICE ORGANIZATION	SUMMARY OF SERVICES PROVIDED	EXPECTED COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS
AWS (Amazon Web Services)	Infrastructure hosting	The external connectivity points to AWS' computing environment should be restricted to the level of network access that is required.
		The AWS KMS should provide secure key management services. The keys should be issued using strong cryptographic algorithms and be protected in transit and at rest.
		The physical access to the AWS data centers where the System is hosted should be limited to properly authorized individuals only, reviewed on a quarterly basis by appropriate personnel, and revoked within 24h of their deactivation.
		AWS should protect the physical entry points of the data centers where the System is hosted with electronic access control devices, closed-circuit television cameras (CCTV) and electronic intrusion detection systems.
		AWS should securely decommission and physically destroy media such as hard drives at the end of their functional life.
		AWS-owned data centers and third-party colocation service providers used by AWS should have environmental controls in place, including fire detection and suppression systems, HVAC systems, uninterruptible power supplies, and generators that are monitored and maintained to protect computer equipment used for the System.
		AWS provides infrastructure with redundant components accessible across various regions and/or zones to support diverse availability requirements.

SUBSERVICE ORGANIZATION	SUMMARY OF SERVICES PROVIDED	EXPECTED COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS
Cloudflare	Web Application Firewall (WAF) and DDoS Protection products	The external connectivity points to Cloudflare's computing environment should be restricted to the level of network access that is required.
		Sensitive data such as TLS keys and certificates should be protected in transit and at rest using strong cryptographic algorithms.
		Cloudflare's systems should be redundant, and an approved and tested Business Continuity and Disaster Recovery plan should be in place.
Acuant **IDVerse** **LexisNexis** **Mitek** **Validated ID** **Veridas**	Identify verification	Identity verification partners must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. They must protect the communication between the platform and its web services. They are also responsible to protect personal data provided by the platform for identity verification.
Twilio **Upscope**	"Virtual Room" videoconferencing capabilities and co-browsing functionalities	Virtual Room videoconferencing partners must implement appropriate technical and organizational measures to reach a level of security appropriate to the risk. They must protect the communication between the platform and its web services. They are also responsible to protect the video recordings that may contain personal data.
OneLogin	Identify and Access Management	OneLogin must protect the security and confidentiality of submitted OneSpan user credentials.
		OneLogin must protect the availability of their service to help allow OneSpan to continuously log on to their outsourced services.