ONESPAN SAAS SERVICE DESCRIPTIONS

OneSpan SaaS Service Descriptions

- Intelligent Adaptive Authentication
- OneSpan Cloud Authentication
- OneSpan Sign
- Risk Analytics Cloud
- Secure Agreement Automation

Intelligent Adaptive Authentication

1. Definitions
   a. **"Customer Application"** means a web-based, offline, mobile or other software application functionality that is provided by Customer or a third party and interoperates with the Service.
   b. **"Excess Limit Fee"** means the price per Transaction listed for the Product on the applicable Order Document that is charged for Transactions in excess of the Monthly Commitment.
   c. **"Monthly Commitment"** means the number of monthly Transactions committed in the applicable Order Document.
   d. "**Session**" means a period of User activity within the Customer Application. A period is determined by (a) the Customer Application's time limitations as set by the Customer or its licensor, or (b) a User's termination of a Customer Application session. A User's return to the Customer Application after an expired Session constitutes an additional Session.
   e. "**Transaction**" means a unique Session.

2. Product Information

Intelligent Adaptive Authentication ("**IAA**") leverages multi-factor authentication, machine learning-powered risk analytics, and application security to help reduce account takeover fraud. IAA provides real-time analysis of User, device and Transaction data, resulting in a risk score that triggers an automated security workflow in the Customer Application which applies the security workflow for each Transaction. Several features and options are available through IAA which may include (as further described in the IAA Documentation):

- Account takeover fraud detection/prevention
- New account fraud detection/prevention
- Real-time detection of an untrusted device
- Real-time analysis of device risk
- Real-time, continuous monitoring of transaction risks
- Identify new fraud scenarios and suspicious account payees
- Policy configuration to support low, medium and high risk actions
- Case management to create, investigate and update suspicious activity
- Role-based access control via a centralized management console
- Interactive fraud relationship visualization
- Reporting
- Web based API (REST Interface)
- Authentication orchestration
- OneSpan Mobile Security Suite Basic Package (SDK Library) (SDK software library subject to OneSpan's Software license Schedule found at www.onespan.com/software-schedule and the Maintenance and Support Service Schedule found at www.onespan.com/maintenance-and-support)
- Secure User mobile onboarding/provisioning keys
- OneSpan Mobile Security Suite OOB Option (Cronto and Push Notification) (subject to OneSpan's Software license Schedule found at www.onespan.com/software-schedule and the Maintenance and Support Service Schedule found at www.onespan.com/maintenance-and-support)

IAA provides customers with three different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of the current version of IAA
- Subject to the Service Levels

Testing:

- Integration development and testing of the current version of IAA
- Not subject to the Service Levels, security requirements or safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment

Development:

- Development access to functionality planned in the next upcoming major release and regression testing of integrations before the new major release is deployed in production
- Not subject to the Service Levels, security requirements, or safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Development environment

3. Pricing

(a) Pricing for IAA is based upon the Monthly Commitment.

(b) Transactions processed in excess of the Monthly Commitment will be charged Excess Limit Fee. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.

(c) Unused Transactions do not carry over to the next month.

4. Additional Service Conditions: Supplier shall encrypt Data in the Service. Supplier may, during the Term, place the Data in a backup location within the System. Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in an applicable Order Document.

OneSpan Cloud Authentication

1. Definitions
   a. **“Excess Limit Fee”** means the price per Transaction listed for the Product on the applicable Order Document that is charged for Transactions in excess of the Monthly Commitment.
   b. **“Monthly Commitment”** means the number of monthly Transactions committed in the applicable Order Document.
   c. “**Transaction**” means an individual API request for authentication (User or Transaction).

2. Product Information

OneSpan Cloud Authentication (“**OCA**”) leverages OneSpan multi-factor authentication to provide both User and Transaction authentication. OCA provides a real-time validation of a OneSpan authentication credential used for either User or Transaction authentication through a REST API interface. Several features and options are available through OCA including, but not limited to (as further described in the OCA Documentation):

- REST API to perform User authentication and Transaction signature validation
- REST API to perform device and User administration
- Centralised management interface for Users and authenticators
- OneSpan Mobile Authenticator Studio (subject to OneSpan’s Software license Schedule found at www.onespan.com/software-schedule and the Maintenance and Support Service Schedule found at www.onespan.com/maintenance-and-support)
- Secure User mobile onboarding and activation

OCA provides customers with three different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier’s discretion.

Production:
- Production usage of the current version of OCA
- Subject to the Service Levels

Testing:
- Integration, development and testing of the current version of OCA
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment

Development:
- Development access to functionality planned in the next upcoming major release and regression testing of integrations before the new major release is deployed in production
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Development environment

3. Pricing
   a. Pricing for OCA is based upon the Monthly Commitment.
   b. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
   c. Unused Transactions do not carry over to the next month.

4. Additional Service Conditions:
   a. Supplier shall encrypt Data in the Service.
   b. Supplier may, during the Term, place the Data in a backup location within the System.

c. Upon Customer’s request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in the applicable Order Document.

OneSpan Sign

1. Definitions
    a. **“Annual Commitment”** means the number of annual Transactions committed in the applicable Order Document.
    b. **“Completed Transactions”** means any Transaction listed as “Completed” or “Archived” on the OneSpan Sign application dashboard.
    c. **“Document”** means a single file representing a form, document or other record, not to exceed 10 megabytes of Data (the “**Document Limit**”), and capable of being viewed, electronically signed, sent or received or stored through the Service. Any Documents in excess of the Document Limit will create one or more additional new Documents, for which Customer will pay an additional Document Fee, where applicable.
    d. **"Excess Storage Fee”** means the fee charged for storage of Complete and Incomplete Transactions in excess of the Fair Use Policy.
    e. **"Fair Use Policy”** means:
        - for all plans, a maximum of 100 signatories per Transaction are allowed, signatories in excess of this amount create an additional Transaction.
        - for Professional plans
            - One thousand (1,000) Transactions per Customer per annual term; and
            - Incomplete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction creation date; and
            - Complete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction completion date.
        - for Enterprise plans:
            - Incomplete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction creation date; and
            - Complete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction completion date.
    f. **“Incomplete Transaction”** means any Transaction that is not listed as a Completed Transaction on the OneSpan Sign application dashboard.
    g. “**Named User**” means Customer’s employee or agent who has been given login access credentials to the Account by the Administrator for purpose of accessing the Service. A Named User must be identified by a unique email address and user name, and two or more persons may not use the OneSpan Sign Service as the same Named User.
    h. **“Overage”** means the price per Transaction listed for the Product on the applicable Order Document that is charged for Transactions in excess of the Transactions committed for an annual term.
    i. “**Transaction**” means a container or package associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the “**Transaction Limit**”). Any Documents in excess of the Transaction Limit will create one or more additional new Transactions, for which Customer will pay the Transaction Fee indicated in the applicable Order Document.

2. Product Information

OneSpan Sign is a software platform for creating and managing the execution of digital transactions with electronic signing and delivery of Documents. Several features and options are available through OneSpan Sign which may include (as further defined in the OneSpan Sign Documentation):

- A 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 Users.

- Transaction management features for preparing and sending documents manually through the user interface or using 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 and both the electronic evidence and summary are protected by digital signing.
- A REST API along with Java and .Net SDKs to allow integrating third-party and custom applications with the Service.
- Support for native mobile applications and pre-built connectors to applications such as Salesforce and Microsoft Dynamics.

OneSpan Sign provides customers with two different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of the current version of OneSpan Sign;
- Documents are not watermarked;
- Subject to the Service Levels.

Sandbox (Staging):

- Integration, development and testing of the current version of OneSpan Sign;
- Documents are watermarked to make them unsuitable for production usage;
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Sandbox environment.

3. Pricing
   a. **OneSpan Sign Enterprise:**
      i. Pricing for OneSpan Sign Enterprise is based upon the Annual Commitment.
      ii. Customer's use of the System is not blocked beyond the Annual Commitment. For use in excess of the Annual Commitment, Customer agrees to pay the Overage fees.
      iii. Unused Transactions in an annual term may not be carried over to the next annual term.
      iv. Transactions stored in excess of the Fair Use Policy shall be charged the Excess Storage Fee invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Storage Fees over more than one quarter prior to invoicing for administrative convenience.
   b. **OneSpan Sign Professional**:
      i. Pricing for OneSpan Sign Professional is based on the number of individual Named Users for an unspecified number of Transaction recipients subject to the Fair Use Policy.
      ii. For use in excess of the Fair Use Policy, Customer agrees to pay the Excess Transaction and Storage Fees.
      iii. Unused Transactions in an annual term may not be carried over to the next annual term.
      iv. Transactions stored in excess of the Fair Use Policy shall be charged the Excess Storage Fee invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Storage Fees over more than one quarter prior to invoicing for administrative convenience.
4. Service Conditions
   a. Customer maintains sole control over the content, quality, and format of any Document, and other than Supplier's obligation to provide the Services as set forth herein, Supplier assumes no

liability or responsibility for a User’s failure or inability to electronically sign any Document or within any particular period of time;

b. Supplier shall not be considered a party to any Document, and Supplier makes no representation or warranty regarding any Document, transaction, agreement or contract sought to be effected or executed using the Service; and

c. Customer is solely responsible for ensuring that any particular Document can be legally executed or formed by electronic signature procedures available through the Service.

Risk Analytics Cloud

1. Definitions
    a. **“Customer Application”** means a web-based, offline, mobile or other software application functionality that is provided by Customer or a third party and interoperates with the Service.
    b. **“Excess Limit Fee”** means the price per Transaction listed for the Product on the applicable Order Document that is charged for Transactions in excess of the Monthly Commitment.
    c. **“Monthly Commitment”** means the number of monthly Transactions committed in the applicable Order Document.
    d. “**Session**” means a period of User activity within the Customer Application. A period is determined by (a) the Customer Application’s time limitations as set by the Customer or its licensor, or (b) a User’s termination of a Customer Application session. A User’s return to the Customer Application after an expired Session constitutes an additional Session.
    e. “**Transaction**” means a unique Session.

2. Product Information

Risk Analytics Cloud (“**RAC**”) analyzes vast amounts of mobile, Customer Application, and Transaction data in real time to detect known and emerging fraud in the online and mobile banking channels including account takeover, new account fraud, mobile fraud, and digital banking fraud. RAC produces a transaction risk score that drives intelligent workflows that trigger immediate action based upon pre-defined and/or Customer-defined security policies and rules. Several features and options are available through RAC which may include (as further described in the RAC Documentation):

- Account takeover fraud detection/prevention
- New account fraud detection/prevention
- Real-time detection of an untrusted device
- Real-time analysis of device risk
- Real-time continuous monitoring of transaction risks
- Identify new fraud scenarios and suspicious account payees
- Policy configuration to support low, medium and high risk actions
- Case management to create, investigate and update suspicious activity
- Role-based access control via a centralized management console
- Interactive fraud relationship visualization
- Reporting
- Web based API (REST Interface)

RAC provides customers with three different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier’s discretion.

Production:
- Production usage of the current version of RAC;
- Subject to the Service Levels.

Testing:
- Integration development and testing of the current version of RAC;
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment.

Development:

- "**Development**" access to functionality planned in the next upcoming major release and regression testing of integrations before the new major release is deployed in production;
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Development environment.

3. <u>Pricing</u>
   a. Pricing for RAC is based upon Monthly Commitment.
   b. Transactions processed in excess of the Monthly Commitment will be charged Excess Limit Fees. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
   c. Unused Transactions do not carry over to the next month.

4. <u>Additional Service Conditions</u>: Supplier shall encrypt Data in the Service. Supplier may, during the Term, place the Data in a backup location within the System. Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in an applicable Order Document.

Secure Agreement Automation

1. Definitions
   a. **"Annual Volume Commitment"** means the annual Component volume commitments as indicated in the applicable Order Document.
   b. **"Excess Limit Fees"** are fees charged at the Component fee listed for each particular Component used in excess of the Annual Volume Commitment.
   c. **"Transaction"** means a Workflow initiated by Customer in the Service for a particular User(s) and is comprised of one or more Components.

2. Product Information

Secure Agreement Automation ("**SAA**") incorporates the Components necessary to facilitate the automated verification of a User's identity and the execution and electronic signing of agreements. SAA is deployed with a single integration, allowing customers to specify only the features they require. Several options are available for configuration by working with OneSpan Professional Services (subject to the Professional Services Schedule at www.onespan.com/professional-services), which may include:

- Configurable Workflows: Customer works with Supplier's Professional Services to combine workflow components in multiple ways (a "**Workflow**")
- Digital Identity Verification: Digital identity verification utilizing the Services' identity document verification Component ("**Identity Document Verification**") or combining this with facial comparison of a 'selfie' (and liveness detection) with the photo from the identity document ("**Identity Document Verification with Face**") and/or its one-time-passcode ("**OTP**") Component .
- E-Signature: Customer may use the Service to capture a User's signature or consent on multiple documents with electronic signing and delivery
- End-to-End Audit Trail: The Service collects complete audit trails, from verification to electronic signature, showing what the User saw and did at each stage of the workflow
- Notifications: Service allows Customer ability to subscribe to several notifications to track User progress through the Workflow
- Localization: Workflow configuration can be defined for many languages; Customer decides the languages required and specifies the text to use so that Transactions are presented in the language requested
- White-Labelling: Allows Customer to customize language and branding, dialog boxes, buttons and navigation
- Responsive design: User interface adjusts for web-browsers on desktop, tablet and mobile devices
- Data Retention: subject to storage limitations, Customer controls incomplete and completed Transaction storage periods and may erase Transactions at any time.

SAA provides customers with two environments to support their integration, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of Workflows on the current version of SAA
- A/B testing may be performed here
- Subject to the Service Levels and subscription Fees

Staging / Testing and Development:

- Integration development, system integration testing of Workflows on the current version of SAA
- Not subject to the Service Levels and data security requirements; as such, Customer acknowledges that no production Data will be uploaded to the Staging/Testing and Development environment, unless Supplier and Customer agree in writing otherwise.

3. Pricing
   a. Pricing for SAA is based upon the Annual Volume Commitment.
   b. SAA Components are priced as follows:
      i. **Platform Component**: Fee assessed once for each Transaction at the time of Transaction creation.
      ii. **eSignature Component**: Fee assessed for each eSignature Component included in a Transaction. Fee charged at the time of Transaction completion. Incomplete Transactions are not charged eSignature Component fees. One Transaction may have multiple eSignature Component fees.
      iii. **Identity Document Verification Component**: Fee assessed for each Identity Document Verification request attempt made by a User at the time the attempt is made within the Transaction.
      iv. **Identity Document Verification with Face Component:** Fee assessed for each Identity Document Verification with Face request attempt made by a User at the time the attempt is made within the Transaction (there are no additional charges for liveness detection).
      v. **OTP Component**: Fee assessed for each OTP attempt made by a User at time the attempt is made within the Transaction. One Transaction may have multiple OTP Component Fees.
   c. Components processed in excess of the Annual Volume Commitment are charged Excess Limit Fees. Excess Limit Fees are invoiced on the annual anniversary in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one annual period prior to invoicing for administrative convenience.
   d. Unused Annual Volume Commitment does not carry over to the next year.

4. Additional Service Conditions
   a. Supplier shall encrypt Data in the Service. Supplier may, during the Term, place the Data in a backup location within the System. Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in an applicable Order Document.
   b. Document Identity Verification Component Terms: Customer may elect to deploy Document Identity Verification Components within the Service. The following terms apply to such deployment by Customer:
      i. Customer will: (i) only use Document Identity Verification for internal business purposes and for the Transaction in which it was initially requested; and (ii) will safeguard and maintain the confidentiality of and restrict the use of any Document Identity Verification disclosed to Customer to the purposes for which its intended.
      ii. Notwithstanding anything to the contrary in the Contract, Supplier:
         (a) will apply only those Document Identity Verification measures (if any) selected by Customer,
         (b) makes no representations or warranties regarding: (i) the appropriateness of such Document Identity Verification, (ii) whether Users have the necessary knowledge or ability to successfully meet such Document Identity Verification measures, or (iii) the

accuracy or validity of the results generated by the Service or the authenticity of any image submitted, and

(c) assumes no liability or responsibility for the circumvention by any User or other person of any Document Identity Verification measures.