ONESPAN FRAUD RISK SUITE DEVICE ON-PREMISE STARTER PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	114
Expected Project Duration	Three (3) months
Location of Professional Services	Remote

2) Governing Terms

The Professional Services are delivered pursuant to the Master Terms available for review at www.onespan.com/master-terms, including the Professional Services Schedule at https://www.onespan.com/professional-services (the "PS Schedule"), unless Customer has previously executed a written agreement for the sale of the Services, in which case such agreement shall control (the "Contract"). Terms not defined herein shall have the meaning given them in the Contract.

3) Assumptions and Pre-requisites

a) This OneSpan Fraud Risk Suite ("FRS") **Device On-Premise** Starter Package (the "Package") governs Supplier's provision of Professional Services aimed at introducing and enabling Customer to implement the OneSpan Fraud Risk Suite (FRS) for Device using an on-premise setup. This Package supports a setup to a maximum of up to five (5) integrated client devices (either mobile application and/or web application).
b) If Customer's requirements exceed those agreed to in this Package, Customer may enter into a Tailored Services SOW (as defined in the PS Schedule) with Supplier instead of this Package.
c) The scope of this package covers one (1) complete project life cycle including:
   i) Solution Design
   ii) On Premise Containerized environment set up
   iii) Competency development
   iv) Guidance during development and test cycles
   v) Go live Support
d) Packaged Services are performed remotely and during standard business hours of the Supplier office providing the Service ("Service Hours"), unless otherwise agreed in writing.
e) Supplier can perform services outside of "Service Hours" at an additional expense through a separate agreement.
f) Customer must have valid licenses for the appropriate OneSpan FRS.
g) Customer is deemed proficient at Kubernetes or Helm to support the on-premise containers installation.
h) Customer will establish sufficient access to use Supplier's current remote services capability.
i) Customer team must be able to provide input regarding the current use cases, business flows and IT architecture for authentication, transaction approval, customer registration and the planned application architecture
j) Customer commits to the dedicated project availability of the following profiles: Project Manager, Enterprise/Security Architect, Fraud Strategy Lead, Product Owner, Mobile Developer, Backend Developer, Business Tester, Fraud Monitoring Analyst.
k) Customer team to perform the development and integration activities between the FRS solution and Customer web and mobile devices and backend.

4) Services

a) Project Management
   i) Supplier will assign a Project Manager during the complete project life cycle to handle coordination and execution of OneSpan related activities/deliverables within time, scope and cost. The project manager will coordinate resource availability and handle dependencies between Customer and OneSpan.
b) Project Kickoff Call
   i) Supplier will conduct a project kickoff call to set objectives and explain project phases and scope.
   ii) Supplier will work with the Customer to see that all prerequisites and requirements conditional for the provisioning of the Services are fulfilled.
c) FRS Solution Design Session
   i) Supplier will conduct a solution design session covering:
      (1) Overall solution introduction
      (2) Device risk best practices
      (3) Architectural and security requirements and constraints
      (4) Define web and/or mobile SDK integration approach, architecture, and compatibility with the bank's technology stack
      (5) Suggest best integration approach the banking fraud system and usage of correlation data
      (6) Suggest best approach for device risk detection rules definition

(7) Suggest best approach for on premise deployment and configuration
(8) Supplier will deliver the solution design document.

ii) Customer will:
(1) Validate the solution design with bank's enterprise, security, and compliance architecture.
(2) Define risk detection logic, risk thresholds, and business rules for SDK usage.
(3) Manage and define business requirements, priorities, and acceptance criteria for the SDK deployment.

d) FRS On Premise Environments Setup And Configuration
(1) For On Premise Cloud Supplier will: work with the Customer to deploy the FRS solution in new testing ("STAGING") and production ("PROD") on premise environments and ensure that they can access and administer this setup.
(2) Customer will prepare
(a) Kubernetes or Helm servers for both environments (STAGING and PROD)
(b) set up test accounts for Supplier validation

e) FRS Competency Development
i) Supplier will
(1) Provide FRS Portal instructions
(2) Provide FRS Mobile and/or Web SDK API Integration competency development to the Customer.
(3) Provide competency development on the integration of risk scoring into the Customer's backend system(s).

f) Guidance During Development And Integration
i) Supplier will:
(1) Deploy the device(s) risk ruleset(s)
(2) Provide technical guidance, SDK documentation, sample code, and troubleshooting support.
(3) Help validate the correct integration between SDK data and fraud decisioning backend or analytics systems
(4) Advise on best practices for the build pipeline and SDK updates

ii) Customer will:
(1) Integrate the client SDK into mobile apps and/or web platforms and handle configuration and development testing.
(2) Ensure correct integration between SDK data and fraud decisioning backend or analytics systems.

g) Guidance During Testing
i) Supplier will:
(1) Provide guidance in support of the Customer's efforts to test with the FRS platform for a period of fifteen (15)-calendar days from the completion of the Engineering Guidance During Integration activity
(2) Provide guidance in an efficient testing approach and help validate fraud event data and performance

ii) Customer will:
(1) Define and execute test plans (unit, integration, UAT) and validate fraud event data and performance
(2) Validate fraud scenarios and confirm risk scoring accuracy before go-live

h) Go-Live Support
i) Supplier will:
(1) Help release to Production
(2) Provide post-go-live support and SDK updates to the Customer for a period of five (5) Calendar days
(3) Arrange for a handover to OneSpan Customer Support

ii) Customer will monitor fraud alerts and performance post-deployment and tune thresholds

5) Project Deliverables

Deliverable #	Deliverable Description
0001	Solution Design
0002	Two (2) configured FRS on premise environments (STAGING and PROD)
0003	Competency development instruction materials

6) Exclusions

a) Configuration of, or for, third party applications or hardware
b) Activities related to Fraud Risk Suite Behavior
c) More than five (5) integrated clients (either mobile application or web application). iOS and Android are considered as two different applications.
d) New Product feature development or customization
e) Recurring consulting for ruleset refinement (available under a separate agreement)
f) Publishing (support) of the mobile application
g) Audit report
h) Custom development
i) Creation of custom documentation or custom training materials
j) Translations (All documents will be in English)
k) Mobile or web banking application development