ONESPAN FRAUD RISK SUITE BEHAVIOR SAAS STARTER PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	256
Expected Project Duration	Six (6) 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") Behavior SaaS Starter Package (the "Package") governs Supplier's provision of Professional Services aimed at introducing and enabling Customer to implement the ThreatFabric Fraud Risk Suite ("FRS") for Device and Behavior provided by OneSpan using the ThreatFabric SaaS.
b) This Package supports a setup to a maximum of up to five (5) integrated client devices (either mobile application and/or web application).
c) 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.
d) The scope of this package covers one (1) complete project life cycle including:
   i) Solution Design
   ii) Cloud environments set up
   iii) Competency development
   iv) Guidance during development and test cycles
   v) Go live Support
   vi) Behavior models training
e) Packaged Services are performed remotely and during standard business hours of the Supplier office providing the Service ("Service Hours"), unless otherwise agreed in writing.
f) Supplier can perform services outside of "Service Hours" at an additional expense through a separate agreement.
g) Customer must have valid licenses for the appropriate ThreatFabric FRS product.
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 must provide appropriately skilled personnel to integrate SDKs within four (4) weeks of the implementation start date.
l) Customer must request or enable appropriate application-level permissions for the proper functioning of the FRS SDKs.
m) Customer must have the ability to phase the rollout of new features through application release cycles.
n) Customer must provide correlation data (e.g., a pseudonymized user ID, session ID, or device ID) to link detection events to customers.
o) 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 and behavioral risk best practices
   (3) Architectural and security requirements and constraints
   (4) Define web and/or mobile SDK integration approach, architecture, and compatibility with the Customer's technology stack
   (5) Suggest best integration approach for the Customer's fraud system and usage of correlation data
   (6) Suggest best approach for device and behavior risk detection rules definition
   (7) Suggest best approach for SaaS deployment and configuration
   (8) Supplier will deliver the solution design document.

ii) Customer will:
   (1) Validate the solution design with Customer's enterprise, security, and compliance architecture.
   (2) Define fraud 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 SaaS Environments Setup And Configuration
   i) Supplier will:
      (1) Assist Customer in generating security certificates necessary to gain access to the public FRS SaaS testing ("STAGING") and production ("PROD") environments.
      (2) Work with the Customer so they can access and administer their STAGING and PROD environments.

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) Deploy behavior model building pipeline(s)
      (3) Provide technical guidance, SDK documentation, sample code, and troubleshooting support.
      (4) Help validate the correct integration between SDK data and fraud decisioning backend or analytics systems.
      (5) 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 End User 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) FRS Device 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 device fraud alerts and performance post-deployment and tune thresholds.

i) FRS Behavior AI models Training
   i) During a maximum period of three (3) months the FRS behavior AI models will be trained using Customer Production data
   ii) Customer will provide feedback regarding specific events that have occurred and can be used for specific model training
   iii) Supplier data scientist will interpret this information and Customer feedback to further improve the models

j) FRS Behavior Go-Live Support
   i) Supplier will help release to Production
   ii) Supplier will provide post-go-live support during a period of five (5) calendar days.

5) Project Deliverables

Deliverable #	Deliverable Description
0001	Solution Design

0002	Two (2) deployed and configured FRS cloud environments (Staging and PROD)
0003	Competency development instruction materials

6) Exclusions

The following are excluded from these Packaged Services:

a) Configuration of, or for, third party applications or hardware
b) Products installed on premise or on private cloud
c) More than five (5) integrated clients (either mobile application or web application). iOS and Android are considered two different applications.
d) Development of any new Product features or functionality not expressly described in the Documentation in effect at the time of purchase
e) Testing automation of Behavior LLM
f) Recurring consulting for ruleset refinement (available under a separate agreement)
g) Publishing (support) of the mobile application
h) Audit report
i) Custom development
j) Creation of custom documentation or custom training materials
k) Translations (all documents will be in English)
l) Mobile or web banking application development
m) Any Professional Services not expressly addressed in this Package