Rapid Response Retainer Professional Service Description
Retail Health Check

1. **Scope of Work.**
   1.1 **Retail Health Check.** The Project consists of a retail health check (the "Professional Services"). Verizon will conduct an investigation at the Customer store locations identified in the Engagement Letter (the "Locations"), to test for evidence of a security breach. The Professional Services will consist of two phases of examination and a third phase providing knowledge transfer to Customer.
      1.1.1 **Phase 1: Onsite Review and Assessment.** During phase 1, Verizon will visit Customer's Locations to discover evidence of a security breach affecting Customer's payment card processing and/or Sensitive Data. "Sensitive Data" consists of:
         - Credit card numbers
         - Credit card track data
         - Other Customer data, subject to mutual agreement.

      1.1.1.1 Major activities in this phase will consist of systems and network inspection, evidence collection, disk and memory analysis, and review of select other types of material evidence, which may include:
         1.1.1.1.1 Forensic imaging of point of sale ("POS") devices, from a sampling of store locations as determined by Verizon;
         1.1.1.1.2 Analysis of a sampling of system memory modules to identify unauthorized processes that may be running and evidence of potential malware;
         1.1.1.1.3 Examination and correlation of active network connections and data transfer flows involving POS systems for evidence of potentially malicious activities;
         1.1.1.1.4 Examination of system process information to identify potentially malicious tampering with authorized transaction related processes;
         1.1.1.1.5 Review to identify suspicious log activity with POS;
         1.1.1.1.6 Review of system scheduled processes to identify potential malware persistency and unusual activity;
         1.1.1.1.7 Performance of registry analysis of Customer's Windows systems to identify possibly embedded malware and unauthorized software; and
         1.1.1.1.8 Analysis of the master file table for created known files exhibiting unusual or out of place characteristics.

      1.1.1.2 To minimize impact to Customer's store operations, material evidence will be collected and preserved from Customer systems and securely transmitted to Verizon's forensics lab to conduct an analysis of collected information.

      1.1.2 **Phase 2: Internet Traffic Pattern Analysis.** Verizon will analyze Customer's netflow data (as identified in the CIP Schedule and further described in the Engagement Letter) for correlation against Verizon's "indicators of compromise" ("IOC") database. The IOC database is a compilation of data collected by Verizon from internal and external sources.

      1.1.2.1 Verizon will examine the netflow metadata (source and destination IP addresses, source and destination ports), packet count and bytes (in Customer's communications, both inbound and outbound), to detect known threat actors, as well as traffic patterns that are considered malicious.

      1.1.2.2 Verizon will also analyze Customer's log data, as further described in the Engagement Letter, to be provided by Customer in advance.

      1.1.2.3 The Customer's log data (the "Logs") shall include Customer's logs exported from Customer's security information and event management ("SIEM") tool(s) for correlation against Verizon's IOC database for evidence of malicious activity.

      1.1.2.4 Customer will load the Logs to an encrypted drive (to be provided by Verizon) and securely ship the drive to Verizon's forensic lab facility for in-depth analysis. Verizon will work with Customer to maintain proper evidence handling procedures and will establish and maintain appropriate chain of custody documentation for the Logs throughout the lifecycle of the Project.

      1.1.2.5 Log data will consist of Customer data from an internet-facing device and include connection data such as source and destination IP addresses, and other data as reasonably required by Verizon.

      1.1.3 **Phase 3: Knowledge Transfer.** Following the completion of phases 1 and 2, Verizon will combine the results of the analysis conducted during each phase and provide Customer with a summary of findings and recommendations related to the findings that may assist Customer with reinforcing security countermeasures where appropriate (collectively, the "Report"). Additionally, Verizon may provide

Customer recommendations as to how Customer may monitor Customer's remaining infrastructure to identify unwanted activity.

1.2 **Project Management.** Verizon will work with Customer to schedule a kickoff conference call to initiate the Project. Verizon and Customer will collaborate to determine required stakeholders and other attendees and the agenda. During or before the kickoff meeting, Customer shall provide a list of appropriate contact personnel with "after hours" emergency contact numbers, and appropriate on-site authorization documentation (where applicable). As an output of the kick off call is an agreement on the resources, dates, times, and locations for the tasks described.

1.2.1 Customer will appoint a single point of contact or program management team to coordinate the Project activities with Verizon and ensure timely data flow and exchange of information required for execution of the Project within the agreed time frame.

2. **Deliverables and Documentation to be produced by Verizon (if any).** Deliverables are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the Agreement's confidentiality terms. Verizon will provide the Report.

3. **Documentation to be produced by Customer and Customer Obligations (if any).** Delivery of the Professional Services by Verizon is dependent on Customer's performance of the following:
   3.1 Customer will provide Verizon with copies of all configuration information, log files, intrusion detection events, and other data relevant to the Professional Services.
   3.2 Customer will be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and security of stored data.
   3.3 In advance of any on-site work, Customer will also provide Verizon with an understanding of the following regarding the in-scope locations:
   - Store POS infrastructure;
   - Payment card authorization request flow;
   - Store-level architectures and variance by region; and
   - Store and headquarters security architecture related to Customer's PCI environment.

4. **Assumptions (if any).** Delivery of the Professional Services by Verizon is predicated on the following assumptions and conditions:
   4.1 Customer is responsible for the implementation of any changes under this SOW to applications or devices managed by Customer or Customer's service providers.
   4.2 Access to the Customer contacts and resources must be provided by Customer during designated time frames, which will be established during the Project kick-off meeting. The failure to provide this timely access could delay completion of the Professional Services.