Routing Code: PS+
SFDC Oppt. ID: TBD

PROFESSIONAL SERVICES
RANSOMWARE ATTACK SIMULATION SERVICE
STATEMENT OF WORK ID TBD
TO VERIZON PROFESSIONAL SERVICES SERVICE ATTACHMENT

This Statement of Work (SOW) is entered into between the entities identified as, respectively, Verizon and Customer in the related Service Order Form (SOF).

1. **PROJECT DESCRIPTION.** Verizon's Ransomware Attack Simulation service provides a remote assessment of Customer's vulnerability to a ransomware attack through an overt or covert approach using Verizon's proprietary ransomware software tool (Ransomware Tool) (Project).

2. **SCOPE OF WORK**

2.1 **Simulated Ransomware Attack - Overt Approach.** If Customer selects to receive the Ransomware Attack Simulation service through an Overt Approach, Verizon will perform the following activities:

2.1.1 **Ransomware Tool Deployment.** Customer will provide Verizon with credentials to an actual or test account (Account) and remote access to one designated workstation or server on the Customer's network (Endpoint). Verizon will use the Account to attempt to execute the Ransomware Tool on the Endpoint. The Ransomware Tool will encrypt specific files on the Endpoint, and it will either delete or hide the originals. The behavior of the Ransomware Tool will be agreed upon by Verizon and the Customer prior to the start of the engagement. Verizon will monitor the ability of the Ransomware Tool to run on the Endpoint and communicate with a mock payment portal. Verizon will provide Customer with a passphrase to unlock or decrypt any files impacted by the Ransomware Tool.

2.1.2 **Payment Portal Monitoring.** Verizon's mock payment portal will track executions and employee payment attempts. Details such as usernames, hostnames, and IP addresses will be collected and stored by Verizon for tracking purposes. Any other information submitted to the payment portal by the employee, such as name or credit card information, will not be collected or stored by Verizon.

2.2 **Simulated Ransomware Attack - Covert Approach.** If Customer selects to receive the Ransomware Attack Simulation service through a Covert Approach, Verizon will perform the following activities:

2.2.1 **Ransomware Tool Deployment.** Customer will provide Verizon with credentials to an Account and remote access to one Endpoint. Alternatively, Verizon will provide either a physical device (Device) or a virtual machine image (Virtual Machine) prior to the start of the engagement. Verizon will use the Account and Endpoint, Device, or Virtual Machine to attempt to covertly execute the Ransomware Tool on up to ten (10) designated workstations or servers on the Customer's network (Target Systems). The Ransomware Tool will either encrypt files on the Target Systems, or it will present a splash screen without modifying any files. The behavior of the Ransomware Tool will be agreed upon by Verizon and the Customer prior to the start of the engagement. Verizon will monitor the ability of the Ransomware Tool to run on the Targeted Systems and communicate with the payment portal. After deployment, the Target Systems will receive a message that demands payment in order for the employee to prevent loss or gain access to the files. Verizon will provide Customer with a passphrase for Customer to give to its employees to unlock or decrypt any files impacted by the Ransomware Tool.

2.2.2 **Payment Portal Monitoring.** Verizon's mock payment portal will track executions and employee payment attempts. Details such as usernames, hostnames, and IP addresses will be collected and stored by Verizon for tracking purposes. Any other information submitted to the payment portal by the employee, such as name or credit card information, will not be collected or stored by Verizon.

3. **DELIVERABLES.** Verizon will develop and provide Customer with a plan for implementing the Project (Project Plan). The Project Plan will list the approach (Overt or Covert) selected by Customer. At the conclusion of the Project, Verizon will provide Customer with a Simulated Attack Report that details the results and statistics of the simulated ransomware attack activities conducted by Verizon.

4. **SUPPLEMENTAL TERMS**

4.1 **Project Management.** Verizon will designate a project manager to manage the Project activities and the change control process (Project Manager), which includes determining when a change order is required. Customer will designate a single point of contact (SPOC) to coordinate the Project activities with the Project Manager.

4.2 **Project Initiation.** The Project Manager will initiate the Project with a kick-off meeting with the SPOC to discuss and review the Project scope, set Project timelines, identify the Customer materials necessary for Verizon to perform the Project. The Project Manager and the SPOC will ensure timely flow and exchange of information required for execution and completion of the Project within the agreed Project timelines.

5. **FINANCIAL TERMS**

5.1 **Rates and Charges**. Customer will pay the Professional Services Ransomware Attack Simulation service Charges specified in the SOF.