

Appendix E
Attachment 01:
Service Description for the Rapid Response Retainer Service

Service Summary

This Service Description describes Verizon's Rapid Response Retainer Services for incident response and forensic engineering support. The Investigative Response elements outlined below are specific to the planned engagement. There are three parts to the Rapid Response Retainer program: 1) the Rapid Response Annual Retainer which provides SLAs for when Verizon will be onsite and provide phone support, 2) the Incident Response and Forensic Professional service provided pursuant to an Engagement Letter in the event of an emergency scenario and 3) the Additional Service Options.

The **Verizon Rapid Response Retainer Service** described in this document is intended to help Customer prepare for, manage, and respond to Computer Security Incidents which are any occurrences or suspected occurrence of:

1. Hostile action(s), or a threat of hostile action(s), that has the intent to affect, alter, copy, corrupt, destroy, disrupt, damage, or provide unauthorized access to a customer's computer system(s) or computer network(s);
2. Dishonest, fraudulent, malicious, or criminal use of Customer's computer system(s) or computer network(s) by a perpetrator (whether identified or not, and whether acting alone or in collusion with other persons) to affect, alter, copy, corrupt, delete, disrupt, or destroy a computer system and obtain financial benefit for any party;
3. Retention and/or misuse of Customer sensitive information, including financial data, consumer and/or identity-related information, in a manner contradicting with existing organizational, legal, or industry regulations ("Data Retention").
4. Threat of, or actual introduction, implantation, or spread of a corrupting, harmful, or otherwise unauthorized piece of code that infiltrates computer system(s), including a set of unauthorized instructions, programmatic or otherwise, that propagates itself through Customer's computer network(s) such as computer viruses, Trojan horses, worms, and time or logic bombs;
5. An attack on Customer's computer system(s) or computer network(s) that results in the degradation or loss of propriety information or quality of service of computer system(s) or computer network(s) (i.e. denial of service);
6. Any threat or connected series of threats to commit a computer crime, or to introduce, implant, or spread a computer virus, or to adversely affect Customer's reputation or public standing which is believed will involve a demand for funds or property to be paid or delivered (i.e. extortion);
7. Any unlawful taking of Customer's electronic data stored in a computer system, or the electronic data of a third party stored in a computer system for which they are legally responsible (i.e. information theft);
8. Gaining of access to Customer computer system(s), backup tapes, storage media, or computer network(s) by an unauthorized person or persons or an authorized person in an unauthorized manner ("Unauthorized Access").

Rapid Response Retainer Services provides Customer with incident response, and computer forensics support. Once engaged in response to an escalated incident, Verizon's investigative response and forensics personnel will attempt to identify the source of a security breach, attempt to determine its full extent and, where possible, contain the breach. While responding to an incident in which the customer intends to trigger

the retainer, Verizon may:

- Establish a timeline of events and reconstruct the attacks.
- Assist in data collection and provide chain-of-custody.
- Identify the source of the unwanted activity and contain it.
- Identify the tools and methods employed by the attackers.
- Determine the quantities and types of sensitive information compromised.
- Work with the authorities in transitioning case evidence.
- Provide a management report containing the impacts of the investigation and relevant findings.

Depending on the circumstances of the incident and the objectives of the investigation based on customer needs – the above activities may or may not be conducted in whole or in part while on the phone prior, or during the onsite investigation, or after the onsite investigation.

In addition to providing a response to potential incidents, this service also provides Customer with access to a wide range of additional investigative response services that may be selected and engaged at any time. More information on these service options can be found in the sections below.

The Rapid Response Retainer Service includes five (5) seats on the Risk Intelligence Portal which provides Customer with direct online access to critical threat and risk intelligence information as produced by Verizon's risk intelligence team. More information on this service can be found in the sections below.

Service Description and Scope

A. Rapid Response Annual Retainer.

The annual retainer fee for the Verizon Rapid Response Retainer Service in accordance with Appendix C of DIR Contract Number DIR-SDD-2514 includes the following items. Actual expenses are not included in the retainer fee and will be bill separately as incurred.

1. Twenty-four (24) Hours of Upfront Discovery Services or First Responder Training.

Upfront Discovery Services. These services include review of Customer's existing incident response (also known as "IR") capability, systems, platforms, data stores, etc. The Upfront Discovery prepares the IR team to respond to support requests. During this component of the engagement, which may be onsite or via net conference, Verizon will attempt to gain an understanding of the Customer's network infrastructure, electronic asset inventory, and threat profile. The Upfront Discovery constitutes a preliminary IR discovery/gap analysis exercise that may be expanded to constitute a full IR discovery/gap analysis engagement. More specifically, during the Upfront Discovery period, investigators will conduct a review of Customer's policy and process in place, tools, training, and testing initiatives. The Upfront Discovery will provide investigators feedback on enhancements to the Customer's existing capabilities. The Upfront Discovery will be conducted on an annual basis.

First Responder Training. Customer has option to use the hours for First Responder Training. The First Responder Training will train responders to help contain the scene of an incident and properly transition the incident to Verizon's investigative response personnel. The content covered in the First Responder Training will vary based on the maturity of Customer's existing capabilities. Material covered during the first responder training will be defined with customer input.

NOTE: Customer has option to use up to 24 hours for either Upfront Discovery or First Responder Training. Hours cannot be used for other activities and do not carryover to the next year.

2. **Dedicated Investigative Liaison.**

The Dedicated Investigative Liaison provides Customer with a consistent interface to Verizon's investigative response team. All Dedicated Investigative Liaisons serve as active investigators who operate in both proactive and reactive modes within the Customer's IR capability. The Dedicated Investigative Liaison will serve as an alternate escalation point to the toll free hotline, and in most cases, will directly contribute to the delivery of Customer's reactive emergency response and proactive incident response consulting engagements (ie: IR Process Development).

3. **Three (3) hour SLA for phone support.**

In the event of an emergency response scenario, the IR team will call the Customer within three (3) hours of the Customer exercising the escalation channels. The escalation channels include either a call to the toll-free support number or a call to the Dedicated Investigative Liaison. An emergency request will consist of requests that are directly driven by a newly discovered or ongoing security incident within the Customer's network environment. Phone support will be billed on an hourly basis pursuant to Customer's Engagement Letter for the specific security incident.

4. **Twenty-four (24) hour SLA for In-transit Security Engineer response.**

In the event of an emergency response scenario, the IR team will be "in-transit" to customer's Customer premises within 24 hours of execution of the Engagement Letter to assist with an emergency of critical security events. "In-transit" is defined as the investigative response engineer is in the act of traveling to the Customer site. The first step in deploying IR team investigators to the Customer's site during an IR emergency is for the parties to prepare the Engagement Letter (the template of which is attached hereto as **Exhibit A**) to be completed by Verizon and accepted by signature from Customer. The SLA begins upon both (a) Customer's delivery of the executed Engagement Letter to Verizon and (b) Verizon's procurement of all required travel documentation and approvals which shall be in accordance with the Texas Travel Management Program Guidelines.. This provision is in place to requisition the proper Customer approval needed to arrange for travel and in response to the volatility of last minute travel and any visas and/or or other travel-related documents. Note that IR team phone support can be used while the investigative response personnel is in route to Customer's site. All Investigative Response services will be billed on an hourly basis pursuant to the Customer's Engagement Letter for the specific security incident.

5. **Online Risk Intelligence.**

Customer will receive a five (5) seat license access to the Verizon Risk Intelligence Portal. The risk intelligence team acquires threat and risk information from a number of sources, observes trends, and reacts to security and risk-related events. Each member of the risk intelligence team monitors for threats and performs analysis in his or her respective areas of expertise. The Risk Intelligence Portal may be accessed in real-time in the form of several popular informational resource utilities.

B. Incident Response and Forensics Professional Services

In the event of an emergency response scenario, Customer is given priority access to Incident Response and Forensics Professional Services, including phone-based or in-person support at the Customer site as required. Customer can initiate these services by entering into an Engagement Letter which outlines the scope and cost of the services. These services can be purchased for the Rapid Response Retainer in either an upfront block of hours or through time and materials at a set rate. Services will be billed on an hourly basis as set forth in the Engagement Letter for the specific incident, plus actual expenses incurred

during the engagement. If services are purchased on a time and materials basis, Customer will be invoiced on a monthly basis, for services and associated fees/expenses incurred during the month preceding.

The incident response and forensics engineering support capabilities and offerings provided by Verizon are continually being developed. The list of service options below should be considered a snap shot of the manner in which Customer can utilize these services. Customer should work with their account liaison to maintain an up to date list of service options. These options will change from time to time as we develop new capabilities. The incident response and forensics engineering support may be used in any of the following ways:

- **Phone-based Evidence Acquisition and Support:** Verizon will provide Customer with direction on creating copies of evidence over the phone to confirm that such copies are exact images without altering the original source.
- **On-Site Evidence Acquisition and Support:** Verizon will dispatch investigative response personnel to the Customer location to assist in evidence gathering. Verizon will provide hardware and software resources required to perform on-site data collection and forensic imaging.
- **Electronic Data Recovery:** Verizon will attempt to salvage deleted or otherwise unrecoverable data from a variety of different media types. Some examples of deleted data are flat and distributed database files, employee email, financial records, and unsaved device configuration files. Information may be recovered from a variety of storage mediums including, but not limited to, server and desktop hard disks, tape backup, optical media, email information stores, and .pst files. Verizon may attempt to provide support onsite; but in most cases Electronic Data Recovery is provided in a Verizon lab with special tools.
- **Data Recovery:** Verizon will attempt to salvage otherwise unrecoverable data from hard drives or memory modules that have become unstable or have failed to be read due to wear, failure, or sabotage. Information may be recovered from a variety of storage devices including, but not limited to, servers, laptops, desktops, notebooks, netbooks, storage arrays (RAID), external hard drives, and flash memory drives. Supported drive interfaces include SATA, IDE, SAS, SCSI, USB, and NAND (flash) memory. Operating systems may include, but are not limited to, Windows, Mac OS, Mac OS X, Linux, UNIX, and Sun. Verizon may attempt to provide support onsite, but in most cases Data Recovery is performed in a Class 100/ISO 5 Verizon cleanroom using special tools.
- **Secured Evidence Transport:** Verizon will confirm that copies of evidence gathered during an onsite visit are securely transported to Verizon forensic labs or other destination specified by Customer. Verizon will provide Customer with explicit direction on such transport when the Customer gathers the information directly. Appropriate chain of custody documentation will be established and maintained throughout the lifecycle of the engagement.
- **Computer Forensic Analysis:** Verizon may perform forensic analysis of any digital evidence as provided by Customer, law enforcement, or as acquired by Verizon's investigative response personnel. The purposes of this Computer Forensics Analysis is to prove or disprove whether a given system, or network of systems, has been the victim of security breach. If a security breach is confirmed, investigative efforts will focus on identifying the initial point of entry into the system, the source of the intrusion, the tools and methods employed by the intruders, and any data compromised, as well as list of other systems, applications, or third-parties potentially compromised. Computer Forensic Analysis may be provided onsite. In most cases – it is provided in a Verizon lab for more thorough analysis.

- **Policy & Process Baselineing:** Verizon will work with Customer to assess security policies and procedures, both documented, undocumented, and informally-applied, against industry practices and standards. The recommended areas of focus for policy and process baselineing are data retention, data control, and incident response. This is largely performed with the use of interview(s) and review of documentation aimed at identifying Customer needs relative to an incident response program and rightsizing a firm-standard set of policies and procedures in these areas. These types of engagements are more in-depth and extensive than what is covered in Upfront Discovery. Policy & Process Baselineing may be provided onsite or remote.
- **Computer Incident Response Training (CIRT):** The purpose of the CIRT training is to articulate the importance of incident response preparedness and familiarity with industry practices and standards. The training provides real-world examples and case studies for the purposes of knowledge transfer to better help the attendees to understand what to do, and what not to do, in the event of a security breach or compromise of sensitive data. This training is more in-depth and extensive than what is covered in Upfront Discovery. Training topics may be customized depending on customer needs. CIRT Training may be provided onsite or remote.
- **Forensics Training:** The Forensics Training service is intended to establish a working understanding of onsite forensics investigation processes and effective tools of the trade. The Forensics Training will provide attendees with a high level of exposure to forensics processes as well as practical experience with the more commonly used forensics toolsets. Note: Verizon's Forensics Training is intended to be customized around the specific needs of the attendees. Training may be provided onsite or remote.
- **Litigation Support:** Verizon's investigative response personnel will assist Customer counsel upon request. Typically, this consists of identifying targets for subpoenas, and technical advice relating to evidence and discovery. *Note: Expert or fact witness testimony, if requested, will be scoped and priced separately.*
- **Evidence Transition to Law Enforcement:** Verizon's investigative response personnel will assist the appropriate legal entity engaged by the Customer. Typically, this means communicating and cooperating with federal or local law enforcement or regulatory agencies to assist with the matter. Evidence Transition may be provided onsite or offsite depending on the circumstances.
- **e-Discovery:** Verizon's Investigative Response personnel will assist Customer counsel upon request for e-Discovery services. E-Discovery services under the Rapid Response include activities covering the initial phases for an e-Discovery engagement, such as data collection and early case assessment. Analysis, processing, review, and final production may be performed but will be scoped and priced separately from the Retainer.

C. Additional Service Option

The following service option provides additional layers of security to help maintain resources availability. This service can be added to the Rapid Response Retainer Services for an additional fee, or purchased as standalone solution outside this Program. The following option is conducted off Customer premises.

NetFlow Logging

Provisioning, Setup and Initial Discovery: Verizon will confirm the Internet Protocol (IP) networks to be monitored in the program. The Investigative Liaison will attempt to verify the network information provided using public (ARIN, RIPE, APNIC, Google, etc.) resources, and will confirm that all networks are somehow connected to the Customer, as a subsidiary or as

the company itself. IP addresses that are not able to be confirmed cannot be monitored and collected. While the Customer is responsible for providing Verizon with only IP networks or IP addresses that legally belong to them, Verizon will report any discrepancies to the Customer.

Data Collection: The term for the NetFlow Logging option service engagement is a period of thirty (30) days. Data is collected on a rolling basis. Analysis and reporting conducted pursuant to an Incident will use IR hours to complete the work. Should the Customer decide to do a full NetFlow engagement outside of triggering the Rapid Response Retainer, a separate agreement would be drawn up.

Service Procedures and Process

Engagement Process

The Investigative Liaison will reach out to the Customer Point of Contact (POC) to schedule the Upfront Discovery exercise as detailed in the "Service Description and Scope" section of this document after ten (10) business days from signing the Service Attachment. Upfront Discovery may be conducted onsite via netconference by Verizon's investigators depending on Customer needs. If conducted onsite travel and expenses will be billed separately.

Customer initialization of this agreement takes a minimum of ten (10) business days from signature.

Following the Upfront Discovery meeting, Customer may engage their retainer-based service in both emergency and non-emergency modes. All engagements begin with an engagement initiation process. This process takes on average three (3) hours during which engagement objectives, cost in hours, and expected deliverables are defined. Engagement details must be agreed upon and captured in the Engagement Letter which must be approved with signature by Customer's POC prior to any work commencing.

Incident Response Phase

Introduction

The **Incident Response Phase** begins when an incident is first suspected and Customer contacts Verizon through the aforementioned escalation channels. The goal of this phase is to contain and investigate an incident as necessary to bring the affected systems back into a trusted state. A key element in the Incident Response Phase involves data collection in the immediate aftermath of an incident. This phase can take place either onsite or remote.

Approach

Verizon works with the Customer to provide an appropriate response given the specific information at hand.

Methodology

Methodology helps identify areas where the Customer may need assistance, which may include the following:

- **Notification:** Notification includes identifying and alerting the appropriate personnel so that a proper response can be formulated.
- **Assessment:** This phase includes verifying the existence, scope, and business impact of the incident. Data may be collected during this phase which may help assess the severity of the incident and level of response that may be necessary. The analysis of this data may assist the Customer to make appropriate business decisions on how to proceed with the Incident Response process.

- **Response and Acquisition:** This phase includes performing various actions based on the decisions made from the Assessment Phase. Examples may include acquiring data from the affected system(s) for in-depth forensic analysis or increasing network monitoring to gather additional data. During this phase data of evidentiary value may be preserved and collected, chain of custody established, and securely transporting to a Verizon's forensic for further analysis.

Verizon Responsibilities

Verizon may provide advice in the following phases of incident management and response:

- **Analysis:** analysis of relevant data to determine the source of the incident, its cause (program error, human error, or deliberate action), and its effects;
- **Containment:** preventing further data loss, and/ or the effects of the incident from spreading to other computer systems and computer networks in the Customer's environment; and
- **Eradication:** removing instances of identified malware, or unprotected sensitive data so that the affected systems can properly secured and brought back online.

Forensic Analysis Phase

Introduction

During the **Forensic Analysis Phase**, analysis is performed on the data that was acquired during the Incident Response Phase. The analysis may reveal the source of the attack, method of intrusion, the extent of sensitive data compromised and any other details relevant to the investigation. This phase can take place either onsite or remote.

Approach

Verizon uses analysis tools, knowledge of operating systems and file systems, and knowledge of vulnerabilities to identify evidence that can be used to determine the origin and details of the incident.

Methodology

Using data gathered during the Incident Response Phase, an analysis is performed to extract evidence. This is done using a combination of open source, commercially available, and Verizon proprietary tools.

During the analysis, Verizon may use several techniques to identify data including:

- Analysis of allocated and unallocated files and directories;
- Timeline of file, application, and network activity;
- Analysis of unallocated file system space;
- Analysis of binaries to identify malicious code, determine its source and capabilities; and
- Analysis of file system structures to find evidence of anti-forensics activities.

Customer Responsibilities

The Customer agrees to:

1. Provide Verizon with copies of all configuration information, log files, intrusion detection events, and other supporting information required for the purposes of the investigation;
2. Manage the collection and dissemination of all information regarding an Incident with the Customer's technical and managerial personnel, legal and public relations departments, others within the Customer's enterprise, and other companies;

3. Be responsible for and facilitate all communications between the Verizon Investigative Response team personnel and any third-party vendors, including Internet service providers and content-hosting firms, used by the Customer to implement an Internet presence;
4. Provide a secure office or work area equipped with desks, chairs, telephones, and laptop computer connections (or analog telephone lines, as Verizon specifies) for use by the Verizon Investigative Response team personnel while working on project premises;
5. Provide the Verizon Investigative Response team personnel with supervised access to computer systems and computer networks during the hours agreed upon;
6. Be responsible for the decision to implement (or not to implement) Verizon recommendations, the actions taken to do so, and the results achieved from such implementation; and
7. Be responsible for data content, as well as the use and implementation of security and access controls.

Verizon Responsibilities

Verizon will designate and provide Customer with telephone and electronic mail contact information for Verizon Investigative Response personnel, obtain answers to Customer security-related questions, and assist the Customer as required. In addition, the Customer may elect to have a Verizon Investigative Response personnel on-site at the Customer premise to assist and perform the duties described above.

Deliverables

At the conclusion of the engagement, Verizon will provide Customer with a Management Report containing the specific findings of the investigation. Depending upon the nature of the engagement, Verizon may produce a Statement of Preliminary Finding(s) as well as a final Management Report.

RAPID REPONSE RETAINER SERVICE DESCRIPTION

EXHIBIT A – ENGAGEMENT LETTER TEMPLATE

Rapid Response Retainer

Engagement Letter is being issued pursuant to <AGREEMENT> signed by Customer for Verizon Services (specifically the “Rapid Response Retainer Service”).

Engagement ID:

RE: Engagement Letter

Pursuant to a request from Customer, under the terms of their Rapid Response Retainer contract referenced above.

Service Location:	
Scope of Work:	
Deliverable:	
Engagement Start Date:	
Hours:	

Verizon Point of Contact	Customer Point of Contact

CUSTOMER SIGNATURE

Authorized Signature:

Name (print):

Title:

Date:

THIS DOCUMENT MUST BE SIGNED BY AN AUTHORIZED CUSTOMER REPRESENTATIVE PRIOR TO ANY WORK COMMENCING FOR THE SERVICES OUTLINED HEREIN. A COPY OF THIS ENGAGEMENT LETTER SHALL BE RETAINED ALONG WITH THE AGREEMENT.