JOINT INFORMATION BULLETIN

Orange County Intelligence Assessment Center

(U//LES) Steps to Identify Individuals Making Threatening Phone Calls

17 May 2017

(U) Overview

(U//LES) Individuals can use various methods of concealment tradecraft to place threatening phone calls. Such concealment tradecraft can present challenges for law enforcement investigators when attempting to identify the individuals. Tactics include the use of voice over internet protocol (VoIP) services, spoofing services, and virtual currency to conceal the caller's identity. Timely legal process to obtain all relevant information about the individuals is imperative for investigators to identify the caller.

(U) Investigative Opportunities

(U//LES) Individuals making threatening phone calls are susceptible to carelessness, which can leave evidence leading to their true identity:

- (U//LES) The individual's email account may be used to create a social media or mobile messaging account in their name
- (U//LES) The individual may use an old or pre-existing email account as a "recovery email account" when creating new email accounts. The recovery email account could lead to additional identifiers which may reveal the subject's true identity

(U//LES) Initial investigation into threat calls typically lead to spoofed phone numbers and proxy IP addresses. The investigation should not be closed when such information is encountered. Additional investigation can possibly reveal historic email addresses, phone numbers, social media accounts, or mobile messaging accounts from a time when the individual may not have employed tradecraft or was careless in concealing their identity. Investigators who continue to collect information belonging to the person will likely discover additional identifiers which could lead to the person's true identity.

(U) Tradecraft Example:

(U//FOUO) Individual creates an email account with a false name to then obtain a phone number associated to the false name using a VoIP service.

(U//FOUO) The individual then uses the VoIP service to place a call to a spoofing service, which generates a new phone number and may modulate the caller's voice. The individual uses Bitcoin or another virtual currency to anonymously pay for the service.

(U//FOUO) Using the spoofing service, the individual places a threatening phone call to the victim.

(U//FOUO) The individual may also use proxy IP addresses, virtual private networks (VPNs), or other means to conceal their true IP address throughout the process, further hindering investigations.

(U) Information Gathering - Victims

(U//FOUO) It is necessary to obtain as much detailed information as possible from the victim, when investigating a telephonic threat, including:

- (U//FOUO) Date and time of the telephone call (including time zone) – if multiple calls were received, include the date and time of each call
- (U//FOUO) Caller ID information, including name and phone number displayed
- (U//FOUO) Phone number where the call was received or was routed from
- (U//FOUO) Telephone service provider where the call was received

(U) Information Gathering – Service Providers

(U//LES) It is essential to make detailed requests when making requests to telephone service providers.[1] Investigators should provide the information gathered from the victim to the victim's telephone service provider and should request the following information:

- (U//FOUO) Billing Code or Service ID number where the call originated
  - (U//FOUO) Which may lead to VoIP services, spoofing services, or another telephone and internet service providers
- (U//FOUO) Date, time, and time zone the call entered the telephone service provider's network
  - (U//FOUO) Which is necessary when sending a request to the VoIP service, spoofing service, or telephone and internet service provider identified by the billing code or service ID number
- (U//FOUO) Any payment information, subscriber information, physical address, IP address, or email address associated with the indicated call

(U//LES) If requests identify a VoIP service, spoofing service, or telephone and internet service provider, investigators are encouraged to request any identified services or companies to request additional information. Investigators should request the following information from VoIP services or spoofing services:

- (U//FOUO) Caller or subscriber information, including name, date of birth, physical address, email address, telephone number, social security number, or any other identifying information
- (U//FOUO) Billing code or service ID number where the call originated, if call originated with another service
- (U//FOUO) Date, time, and time zone the call was initiated or entered the service or network
- (U//FOUO) Any payment information, IP address, or other identifying information associated with the indicated call
- (U//FOUO) Type of device used to generate the call
- (U//FOUO) Any other phone numbers called by the caller or subscriber, including date and time (including time zone) of such calls

(U//LES) If requests identify an internet service provider (ISP) or email service, investigators should request the following information from the ISP:

- (U//FOUO) Subscriber information, including name, date of birth, physical address, email address, alternate email address, telephone number, social security number, or any other identifying information
- (U//FOUO) Any payment or billing information linked to the account
- (U//FOUO) All IP addresses from which the account was accessed during a specified time period
- (U//FOUO) Type of device(s) used to access the account

(U//FOUO) Investigators are reminded that depending on the levels of tradecraft used by the individual, multiple rounds of requests may be necessary to discover identifiers which could lead to the person's true identity.

Report threats or suspicious activity to the OCIAC by submitting a tip or lead at:

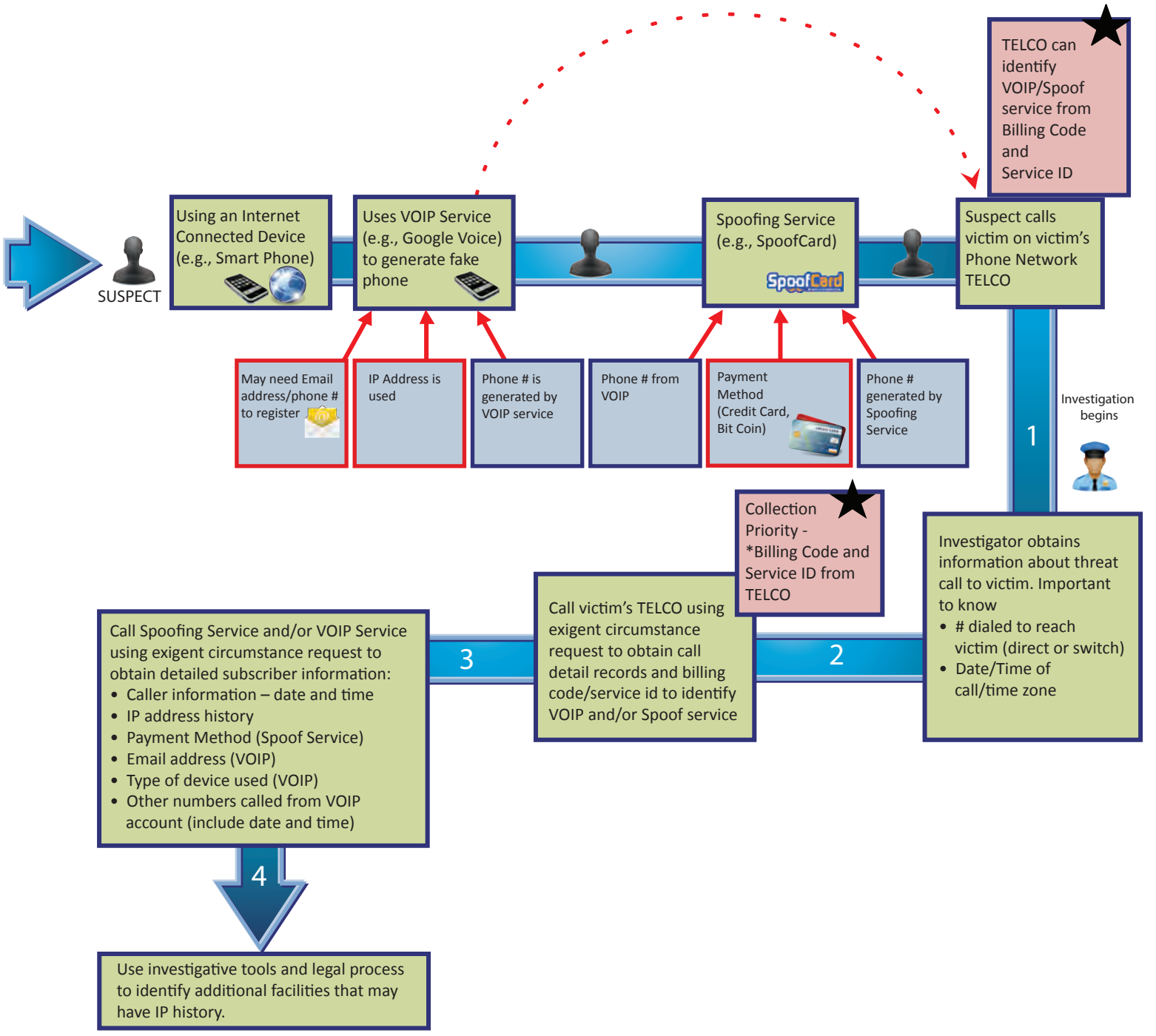
www.OCIAC.ca.gov

(U) Coordinated with FBI Los Angeles – Field Intelligence Group (FIG)
(U) Tracked by: HSEC 1.6, 1.7, 1.8, 1.10, OCIAC I.1.a, III.1

[1] (U//LES) Depending on the severity of the threat or status of the investigation, requests to VoIP services, spoofing services, or telephone and internet service providers may be made using exigent circumstance requests or search warrants. For convenience, exigent circumstance requests and search warrants will be collectively referred to generally as "requests."

(U//LES) Investigative Steps to Identify Individuals Using Communication Tradecraft to Make Threatening Phone Calls

Flowchart from Suspect to Investigation



Key Investigative Objectives

- Use open source (OSINT) tools with known e-mail addresses or telephone numbers to identify additional modes of communication (e-mail, phone numbers, social media accounts, mobile messaging apps).
- Obtain as many IP addresses as possible from the exploitation of those additional modes of communication.
- If investigation leads to a proxy IP address, continue investigation to find a valid IP address with a legitimate Internet Service Provider (ISP).

To report suspicious activity, submit a tip or lead at www.OCIAC.ca.gov or call 714-289-3949