Situational Awareness Report

UNCLASSIFIED//FOR OFFICIAL USE ONLY

New Jersey Phone Kidnapping Scams

8 February 2013

(U//FOUO) NJ ROIC Fusion Liaison & Intelligence Training Unit FLIT 201302-318

New Jersey Kidnapping Scam Summary

(U//FOUO) During recent weeks, various sources in law enforcement and media outlets have been reporting phone kidnapping scams occurring in Central and Northern New Jersey and New York. In most incidents, scammers have alleged that a member of the phone scam victim's family had been involved in a car accident and claimed to have taken the victim's family member hostage. The scammers then claim they will drop their hostage at a hospital after a certain amount of money (usually $1500-2000) is wired via Western Union to the scammers, as restitution for damage to the scammer's vehicle. In addition, the scammers state that they have the hostage's cell phone and any attempts to call the cell phone or disengage from the conversation will result in the murder or beating of the hostage. The scammers try to hold the victim on the phone as long as possible while attempting to persuade them to wire the money; however, reports from some victims indicate the scammers will hang up and not call back under certain circumstances. For instance, when the victim questions the scammers about the hostage's name, the scammers end the call when they are unable to provide the hostage's name. According to Officer Kelly Denham, Coral Gables Police Department (Florida), this scam has been tracked back to 1998, when it started in Puerto Rico. She adds that this scam resurfaces every few years. Over the past few months, the NJ ROIC has seen increased reporting of this scam along the east coast.

Comparisons with Similar Scam Incidents

(U//FOUO) In January 2013, reports indicated a similar scam targeting the elderly. In this scam, elderly grandparents were informed their grandchildren were in prison and that the grandparents needed to wire money immediately to ensure their relative's release. Reports indicate that the scammers may be garnishing information about their victims from Facebook and other social media websites. Several instances of this scam have been reported to local authorities and an alert has been issued throughout the tri-state area. Although there are commonalities among these incidents, the NJ ROIC has received no information indicating that the incidents are connected.

Common Trends

(U//FOUO) Since 2008, the Federal Bureau of Investigations Internet Crime Complaint Center (IC3) has received similar complaints which focus on some common trends for these types of scams throughout the United States.
These include:

- (U//FOUO) The caller/suspect claims to be a relative (usually a young person) who is out of the country and in trouble with the police or a criminal element and needs money wired to him/her to get out of trouble.
- (U//FOUO) The caller/suspect calls back several times demanding additional money be sent in increments of $3000-$4000.
- (U//FOUO) The caller/suspect instructs the victim to go to a Walmart or Money Gram location and wire the money to a person whose name is not the so-called relative.
- (U//FOUO) Sometimes, the caller/suspect will instruct the person to stay on the phone throughout the entire wire transaction. Other times the caller/suspect will instruct the victim not to call the relative's parents because they will worry or be angry.
- (U//FOUO) In another instance, the caller/suspect calls the grandparent/parent and asks for them by name, claiming to be a police officer in another country and instructs the parent on how to get a debit card (amounts are usually under $2000.00) and where to send it for the bail.

How to Prevent the Scam

- (U//FOUO) When family members are going to work, school, and/or out for the day, know their itinerary, who they will be with, where they are traveling to, and what their final destination will be.
- (U//FOUO) Know the cellular telephone numbers of your family members and the subscriber to the respective cellular telephone numbers.
- (U//FOUO) Know the service provider and how to contact the service provider for the respective family members cellular telephone number. This will aid the police with the investigation and further assist with locating the cellular telephone of the family member by "pinging" the respective cellular telephone off various cell sites to determine where the cellular telephone is located.
- (U//FOUO) Constantly update and query your privacy settings on social media profile sites.
- (U//FOUO) Do not provide unknown individuals with your personal information via social media sites and only provide your private information to those you know and/or wish to have that information.
- (U//FOUO) Check to see what privacy information is readily available to the public via the respective social media sites that you and your family are linked to.

What To Do If You Receive Such a Call

- (U//FOUO) Attempt to verify the validity of the number the scammer is calling from.
- (U//FOUO) Attempt to verify the authenticity of the caller of the scam.
- (U//FOUO) Attempt to identify the location of the person and/or family member potentially being kidnapped.
- (U//FOUO) Notify your local police immediately.
- (U//FOUO) Refrain from accepting any subsequent calls from the number associated with the scam.
- (U//FOUO) Ensure you ask specific questions if you are contacted by the party in association with the scam about the suspected "hostage." If there is a lack of specific information furnished by the scammer, this may prompt the scammer to end the conversation.
- (U//FOUO) If you cannot speak with the person and/or family member suspected of being kidnapped and you are unable to locate the person and/or family member suspected of being kidnapped, then call the service provider of the cellular telephone associated with the person and/or family member suspected of being kidnapped. In these emergency situations, the service provided could "ping" the respective cellular telephone in an attempt to locate the person's and/or family member's cellular telephone.
- (U//FOUO) Record the telephone number the suspected kidnapper and/or suspected scammer is calling from.
- (U//FOUO) Save any text messages and/or photographs the suspected kidnapper and/or scammer sends to you.
- (U//FOUO) Lastly, do not panic, think with a clear head, and provide the proper information to your local police assist with the investigation of the incident and/or scam.

Note: (U//FOUO) Be aware of phone "Spoofing," in which a suspected scammer calls from his/her telephone, however has spoofed and/or has masked his/her real telephone number with another telephone number that appears as such on the other party's (victim's) telephone.