



FBI PRESS RELEASE

Salt Lake City Field Office

Federal Bureau of Investigation ♦ 5425 West Amelia Earhart Drive ♦ Salt Lake City, UT 84116

For Immediate Release

Date: August 4, 2021

Contact: Sandra Yi Barker
(801) 579-6400

FBI Warns Public of Extortion Scams Targeting Families in Western Montana

Helena, MT - The Federal Bureau of Investigation Salt Lake City Division, Helena Resident Agency Office, wants to warn the public about virtual kidnapping scams and variations of this type of scam, targeting families in western Montana.

FBI Salt Lake City has recently received reports of victims getting calls from scammers claiming to have kidnapped their loved one and threatening to harm them unless a ransom is paid. No one is physically kidnapped in these schemes, but they are often traumatic for everyone involved. Many of these calls originate in Mexico.

In one recent case, a scammer was able to convince a Kalispell man that his son was in danger and defrauded the victim out of thousands of dollars.

In another case, criminals targeted a woman whose daughter was reported missing earlier this year. The scammers used phishing techniques and information from social media posts to try and convince the woman that the teen was in immediate danger and a ransom needed to be paid for her safe return. The woman did not pay the ransom.

These extortion schemes typically involve an individual or criminal organization who contacts a victim via telephone and demands payment for the return of a “kidnapped” family member or friend. While no actual kidnapping has taken place, the callers often use co-conspirators to convince their victims of the legitimacy of the threat.

Callers, sometimes representing themselves as members of a drug cartel or corrupt law enforcement, will typically provide the victim with specific instructions, to ensure safe “return” of the allegedly kidnapped individual. These instructions usually involve demands of a ransom

payment. Most schemes use various techniques to instill a sense of fear, panic, and urgency in an effort to rush the victim into making a very hasty decision. Instructions usually require the ransom payment be made immediately and typically by wire transfer. These schemes involve varying amounts of ransom demands, which often decrease at the first indication of resistance. The perpetrators will often go to great lengths to engage victims in ongoing conversations to prevent them from verifying the status and location of the “kidnapped” individuals. Callers will often make their victims believe they are being watched and were personally targeted. In reality, many of these callers are outside of the United States, simply making hundreds of calls, possibly using phone directories or other phone lists.

Although the FBI does not keep national statistics of virtual kidnapping for ransom, according to the FBI’s Internet Crime Complaint Center (IC3) in 2020, extortion scams had the third highest victim count in the U.S., behind phishing scams, and non-payment/non-delivery scams. Montana had 186 victims of extortion with losses totaling \$413,176. The FBI believes most virtual kidnappings for ransom remain unreported. We hope to raise awareness about this most recent scheme and equip individuals with the knowledge they need to avoid becoming a victim of this crime.

To avoid becoming a victim of this extortion scheme, look for the following possible indicators:

- Calls are usually made from an outside area code
- May involve multiple phone calls
- Calls do not come from the kidnapped victim’s phone
- Callers go to great lengths to keep you on the phone
- Callers prevent you from calling or locating the “kidnapped” victim
- Ransom money is only accepted via wire transfer service

If you receive a phone call from someone who demands payment of a ransom for a kidnapped victim, the following should be considered:

- Stay calm.
- Try to slow the situation down.
- Avoid sharing information about you or your family during the call.
- Request to speak to the victim directly. Ask, “How do I know my loved one is ok?”
- Request the kidnapped victim call back from his/her cell phone
- Listen carefully to the voice of the kidnapped victim if they speak, and ask questions only they would know.
- If they don’t let you speak to the victim, ask them to describe the victim or describe the vehicle they drive, if applicable.
- While staying on the line with alleged kidnappers, try to call the alleged kidnap victim from another phone.
- Attempt to text or contact the victim via social media.
- Attempt to physically locate the victim.
- To buy time, repeat the caller’s request and tell them you are writing down the demand, or tell the caller you need time to get things moving.
- Don’t directly challenge or argue with the caller. Keep your voice low and steady.

Anyone with information about these fraud schemes is encouraged to contact the Salt Lake City FBI at (801) 579-1400.

FBI Salt Lake City is committed to working with our state and local law enforcement officers to increase public awareness regarding the threat posed by virtual kidnappings and will continue to investigate and refer these types of cases for prosecution.

- For more information on virtual kidnapping for ransom schemes, read here: <https://www.fbi.gov/news/stories/virtual-kidnapping>.
- For more information on scammers targeting families who post missing persons on social media, read here: <https://www.ic3.gov/Media/Y2021/PSA210514>

###