



NEWS RELEASE

For Immediate Release:

February 8, 2024

U.S. Marshals Office of Public Affairs

(703) 740-1699

US Marshals, FBI Urge Public: Report Phone Scams

Spoofers using government phone numbers, government employees' names, demanding payment via bitcoin ATMs

Erie, PA - The U.S. Marshals and the FBI are alerting the public of several imposter scams involving individuals claiming to be U.S. Marshals, court officers, or other law enforcement officials. They are urging people to report the calls their [Local FBI office](#) and file a consumer complaint with the [Federal Trade Commission](#), which has the ability to detect patterns of fraud from the information collected and share that data with law enforcement. Pennsylvania residents are seeing a large number of the scam calls.

During these calls, scammers attempt to collect a fine in lieu of arrest due to a claim of identity theft, failing to report for jury duty, or other civil process issues. They then tell victims they can avoid arrest by making a payment first. Often that means withdrawing cash and transferring it to the government by depositing cash into bitcoin ATMs.

Scammers use many tactics to sound and appear credible. They sometimes provide information like badge numbers, names of actual law enforcement officials, federal judges, and courthouse addresses. They also spoof government phone numbers to appear on caller IDs as if they are calling from a government agency or the court.

The scammer provides identity confirming information to the victim by reading old residential addresses, phone numbers, and other personally identifying information that seem to make their claims legitimate. The scammer then provides a fake personal ID number, case number for the investigation, and warrant number. The call then ends with the scammer advising the victim that they will be recontacted by an investigating official.

A short time later, the victim is contacted by another individual identifying himself as a United States Marshal who is looking into the case. U.S. Marshal for the Western District of Pennsylvania Steve Eberle's name has often been used by the scammers. The scammer reviews the previous conversation the victim had and tells the victim there are two ways to resolve the issue: 1) hire a criminal lawyer to represent the victim or option 2) pay the cash fine.

The victim is instructed to stay on the phone so the conversation can be recorded and used as proof of the victim's compliance. The victim is then instructed to withdraw "80% of their physical assets" and deposit them into a personal digital wallet (Bitcoin) while saving withdrawal receipts and deposit receipts to be reviewed by the investigating official once a meeting can be established. The victim is then told their money will be transferred back to them once the process is completed and the victim will be cleared of any criminal wrongdoing.

To make the scam seem more realistic, the numbers appearing in the caller ID display as the office number of the U.S. Marshals Service, and maybe a specific judicial district. The victim is also instructed to confirm the authenticity of the caller by visiting the USMS website.

The final step in the scam is that the scammer instructs the victim to send a photo of their driver's license to a phone number provided by the scammer. The victim is then instructed to send the QR code scanned at the Bitcoin deposit kiosks.

There have been many victims reporting losses in the thousands to tens of thousands of dollars. The U.S. Marshals Service receives inquiries regularly from victims and potential victims of this scam.

If you believe you were a victim of such a scam, you are encouraged to report the incident to your [local FBI office](#) and to the [FTC](#).

Things to remember:

- The U.S. Marshals Service WILL NEVER ask for credit/debit card/gift card numbers, wire transfers, or bank routing numbers, or to make bitcoin deposits for any purpose.
- NEVER divulge personal or financial information to unknown callers.
- Report scam phone calls to your [local FBI office](#) and to the [FTC](#).
- You can remain anonymous when you report.
- Authenticate the call by calling the clerk of the court's office of the U.S. District Court in your area and verify the court order given by the caller.