Ventura County
SHERIFF'S OFFICE
Jim Fryhoff - Sheriff | **John Reilly** - Undersheriff
800 S. Victoria Avenue, Ventura, CA 93009 | 805.654.2385 |VenturaSheriff.org

Nature of Incident: Phone / Computer Scams - Using Couriers to Collect Cash from Victims

Location: Thousand Oaks

Date: March 2025

Unit(s) Responsible: East County Investigations Bureau

Narrative:

The Financial Crimes Unit in Thousand Oaks has become aware of a recent rash of theft by false pretenses targeting local residents with the use of a courier service. The scammers represented themselves as members of legitimate nationally known businesses. The following is an example of a reoccurring scam affecting innocent victims in the city of Thousand Oaks:

The scam will initially appear via an unsolicited email. The email would portray themselves as legitimate correspondence from companies such as PayPal, Geek Squad and eBay and advise the victim of a fraudulent purchase made on the victim's account. Additionally, the email would offer support to the victim in rectifying the charge. The victim would contact the "representative" via a provided phone number and speak with someone who claimed to be willing to assist them. The phone numbers used in the scam were internet phone numbers created by the scammer and canceled after the scam was completed.

During the commission of the scam, the fraudulent purchase would be processed as a reimbursement to the victim's bank account. As the reimbursement would take place, the scammer would claim they accidentally entered the wrong dollar amount (ex. $15,000 instead of $150.00) and would demand the victim return the overpayment back to the scammer.

In many cases, the scammer had been able to access the victim's bank account prior to the "reimbursement" and move the victim's money from within their own accounts so it would appear to the victim the accidental deposit had occurred. In some cases, the scammer had convinced the victim to download applications that would allow the scammer remote access to the victim's computer. By convincing the victim to provide sensitive personal identifying information (PII) such as user names, passwords, Social Security numbers, etc.) coupled with remote access, the scammer would have access to the victim's bank accounts.

The scammer would direct the victim to go to their banking institution and withdraw the overpayment in cash to return. Since the amount to be withdrawn would be large and raise suspicion from a bank teller, the scammer would advise the victim to tell the teller they needed the money to purchase a vehicle or make home improvements. After obtaining the cash, the victim would be told a "courier" would be arriving at their residence to collect the overpayment. The victim would be given a code word and instructed to ask the courier for the correct code word to confirm the legitimacy of the transaction.

Some scammers will utilize a courier with actual ties to the scam itself. In other cases, Uber and Lyft drivers will be unwittingly hired by the scammer to collect the package (money) from the victim.

Due to the voluntary withdrawal of the funds from their bank, the victims are rarely reimbursed the lost funds even though it was part of a scam.

The Sheriff's Office wants to warn the public of scammers representing themselves as members of legitimate, nationally known companies. No reputable company will make an error of overpayment and not have the ability to recall or fix the error. Furthermore, no legitimate company will request or require anyone to repay "funds in error" via a courier service.

Scammers prey on victims by creating a sense of urgency regarding monetary funds and potential lack of computer knowledge in hopes the victims will make rushed decisions before they have time to realize a scam may be occurring.

Tips to Protect Yourself Against Scams

- Recognize scam attempts and end all communication with the perpetrator.
- Never give unknown, unverified persons remote access to devices or accounts.
- Be cautious of unsolicited phone calls, mailings, and door-to-door service offers.
- Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to unverified people or businesses.
- Resist the pressure to act quickly. Scammers create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.
- Nationally known and legitimate businesses will not demand payment by cryptocurrency, prepaid cards, wire transfers, or overnight mailed cash, or courier services to collect any payments.
- Legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals, nor demand immediate payment or require payment via prepaid cards, wire transfers, cryptocurrency, mailed cash or use courier services.
- Legitimate lotteries and beneficiaries do not need to pay upfront taxes and fees to claim a prize or inheritance. Playing foreign lotteries in any form is a violation of federal law.
- Be careful what you download. Never open an email attachment from someone you do not know and be wary of email attachments forwarded to you.
- Take precautions to protect your identity if a criminal gains access to your device or account.
- Immediately contact your financial institutions to place protections on your accounts and monitor your accounts and personal information for suspicious activity.
- Make sure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls. Disconnect from the internet and shut down your device if you see a pop-up message or locked screen. Pop-ups are regularly used by perpetrators to spread malicious software. Enable pop-up blockers to avoid accidentally clicking on a pop-up.

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.

If you receive a suspected scam call, text or email, we recommend citizens hang up, block the number (if possible), and do not send the scammers any money. If you are unsure or concerned you may be involved in a scam, you can contact your local police station using their official phone number and not the number provided by the suspected scammer. If you are a victim of a scam, please contact the Sheriff's Dispatch non-emergency number at 805-654-9511 to make a report. You can also file a complaint online with the Federal Trade Commission at www.ftc.gov or the Federal Bureau of Investigation at www.ic3.gov.

Prepared by: Detective Jason Cashmark

News Release Date: 03/19/2025

Media Follow-Up Contact: Detective Jason Cashmark (805) 494-8211, jason.cashmark@ventura.org

Approved by: Captain Albert Ramirez

YES ☐ NO ☐

Booking Photo Release:

Ventura County Crime Stoppers will pay up to $1,000 reward for information, which leads to the arrest and criminal complaint against the person(s) responsible for this crime. The caller may remain anonymous. The call is not recorded. Call Crime Stoppers at 800-222-TIPS (8477).

###