CUNA MUTUAL GROUP

Common Member Scams

Each year, fraudsters find new ways to trick people and financial institutions out of money. Whether its an imposter scam – impersonating a love interest, a grandchild, debt collector, etc. – or stealing someone's identity, these fraudsters know how to pull it off. While some of these scams involve new tricks, many have been around for decades.

Using common channels like emails, text, and phone calls; fraudsters typically disguise their identify while retrieving confidential member information.

To no surprise, scammers most commonly request their money through wire transfer – the most common of any payment method reported with a total of $423 million last year.* The Federal Trade Commission also reported a surge of payments connected with gift cards, including reloadable cards.

Consumers reported

$1.48 billion

of fraudulent losses to the FTC *

**The Top Fraud of 2018, Federal Trade Commission*

While it can be difficult to prevent these scams from happening; you can help educate your members on what to look for. Use mitigation tips to ensure your credit union employees are having the right conversations with your members.

Romance

Scammers create fake online dating profiles to lure victims into giving them money.

Phishing, Vishing, SMiShing

Social engineering tactics used to entice recipients to act quickly through spoofed channels.

Secret Shopper

Fraudsters pose as companies offering mystery shopping services to dupe shopper out of money.

Advanced Fee

Victim enticed to wire upfront fees for a fictious promise of receiving a gift of money.

Elderly

Seniors are tricked into sending money to help out their "grandkids" or pay for services.

Common Member Scams

Romance Scams

Using fake online dating profiles with photos of other people to lure their victims, scammers often say they are from the U.S. but are temporarily traveling or working overseas. Some of the fictitious occupations include working on an oil rig, in the military, or as a doctor with an international organization.

The scammers quickly profess their love and tug at the victim's emotions with fake stories and their need for money. They often request money for reasons such as a plane ticket, other travel expenses, and customs fees – all needed to get back into the country. The victims often wire the scammers money never hearing from their "sweetheart" again.

Other variations of this scam include:

- Victims are duped into providing online banking login credentials. The scammer then logs into the account and uses the account-to-account (A2A) / external feature to initiate ACH debits against accounts at other institutions pulling funds into the victim's account for deposit. The victim is instructed to send the funds to the scammer by Western Union or MoneyGram. The ACH debits are subsequently returned to the credit union as unauthorized up to 60 days later.

  According to the Better Business Bureau, up to 30% of those scammed in 2018 were used as money mules, asked to open bank accounts by the scammer so they could send money to the victim for a short period of time. If the account is flagged as suspicious, they will close the account and find another victim. Many of those scammed are embarrassed to report it. If a romance scam is suspected, stop communicating with the scammer and explain your situation to a trusted friend or family member for their advice.

- The scammer logs into the victim's account and requests mobile remote deposit capture service. Once the account is set-up for mobile remote deposit capture, the scammer transmits images of fraudulent checks for deposit to the victim's account. Again, the victim is instructed to send the funds to the scammer by Western Union or MoneyGram. The checks are subsequently returned unpaid.

Phishing / Vishing / SMiShing

Social engineering fraud is range of malicious activities carried out by fraudsters through human interactions. It uses psychological manipulation to trick users into making security mistakes. Unsolicited emails, text messages, and telephone calls purportedly from a legitimate company or individual requesting personal, financial and / or login credentials.

- **Phishing -** One of the most popular forms of social engineering attempts to acquire sensitive information such as usernames, passwords and account or card details by masquerading as a trusted entity and creating a sense of urgency, curiosity or fear in victims. It then prods recipients into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware. Remind members not to click on links or open attachments in emails received from individuals they do not know.

- **SMiShing** - A type of phishing attack where mobile phone users receive text messages containing a website hyperlink; which, if clicked would lead to a malicious URL and/or download malware to the mobile phone. It could appear to come from the recipient's credit union with an intent to gain their personal or account information. In addition, there could be a request to call a fraudulent phone number. Warn members that if they receive these types of texts to call the institution at a number of record, not the one included in the text, to verify legitimacy.

- **Vishing -** Voice phishing is the telephone equivalent of phishing attempting to scam the user into surrendering private information that will be used in identity theft. Often, the call will come from a spoofed phone number making it look like the credit union is calling the member which will provide the member with a sense of legitimacy. Inform members that if they receive this type of call to contact the credit union or whatever business is represented at a number of record, not a callback of the incoming number, to verify legitimacy.

Common Member Scams

Secret Shopper Scams

Members looking to earn extra cash are frequently tricked into participating in the secret shopper scam. If a member accepts the job, he/she receives a counterfeit cashier's check ranging from $2,000 to $5,000. They are instructed to cash the check and purchase money orders and gift cards and send them to the scammers. For their efforts they will keep a percentage of the check they receive. The counterfeit check is subsequently returned unpaid and charged back to the member's account.

Advanced Fee Scams

In the advanced fee scam, the scammer informs a victim that he/she has won a large award (think bogus lottery scam) or is entitled to a large inheritance from a deceased relative. However, before the victim can receive the money, he/she must supposedly pay taxes or fees. The victim ends up wiring funds to the scammer to pay the taxes or fees but never hears from the scammer again.

Elderly Scams

Just as they sound, elderly scams target seniors where the scammer will call a loved one, often a grandparent, pretending to be a grandchild or other relative. They will indicate they have been arrested and need bail money or are at the border and trying to get back into the country and they need money wired to them, usually by Western Union. When receiving these calls, the grandparent is anxious to help their grandchild, but if they call the grandchild at a number of record or other relatives for assistance this scam should be discovered rather quickly. Variations on this scam include an "attorney" calling on behalf of the person in trouble, and instead of wiring funds the request is to purchase gift cards and provide the account numbers.

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com

800.637.2676 | cunamutual.com
P.O. Box 391 | 5910 Mineral Point Road
Madison, WI 53701-0391

CUNA MUTUAL GROUP