TruStage™

Fraud & scams

Member risk overview

Each year, fraudsters find new ways to trick people and financial institutions out of money. While some scams involve new tricks, many have been around for decades. Of the over 2.3 million fraud reports, 26% indicated money was lost. In 2022, consumers reported losing nearly $8.8 billion to fraud.

Fraudsters target the weakest link: humans

Using common channels like emails, text, and phone calls; fraudsters typically disguise their identity while retrieving confidential member information. They use tactics to succeed by tugging at the basic human instincts to trust and please. The scams look to catch your employees off-guard and/or to dupe your members into making security mistakes or giving away sensitive information and money.

No matter the channel, fraudsters are crafty, knowing how to pressure people to make decisions on the spot by using innovative schemes. Their multi-channel approach looks for victims who find their stories convincing and will willingly click on links or share sensitive information, which can be used to authorize and transact many types of transactions.

Scams are often hard to detect at a quick glance; however, these common red flags can help. Keep in mind…it is not uncommon for fraudsters to use intimidation tactics and urgent requests.

As fraudsters get more sophisticated in the ways they exploit technology and humans; it is even more important to know what to look for, to take the right action steps, and remain vigilant. We're all human, after all.

You can report fraud, scams, and other illegal business practices by going to the Federal Trade Commission website **www.ReportFraud.ftc.gov**.

Younger people lost money to fraud more often than older people

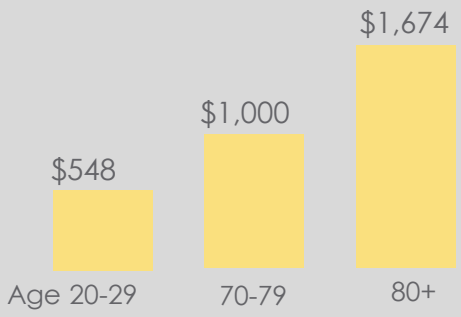
43%

Victims ages 20-29 lost money to fraud

23%

Victims ages 70-79 lost money to fraud

However, people aged 70+ had a much higher median loss



Source: Consumer Sentinel Network Data Book 2022, Federal Trade Commission

Typical fraudster approach

Regardless of the fraud type or intention, fraudsters' first objective is to convince others that they are a real member.

Fraudster's often:

- Build victim profiles
- Change members' contact information
- Request wire transfers and withdraw funds
- Request canceled checks
- Order share drafts
- Request password resets
- Request credit / debit cards
- Set-up audio response or online banking

Fraudsters tend to gravitate to the phone channel because the primary line of defense — call center representatives asking challenge questions — is highly vulnerable to social engineering. It is easier for fraudsters to find answers to challenge questions and then social engineer a rep into granting access to a member account than it is to hack IT infrastructure backed by a dedicated security team.

27 million American consumers are reportedly victimized by identity fraud-related financial losses.

Source: Javelin 2022 Identity Fraud Study "The Virtual Battleground"

Social engineering fraud

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 are common approaches.

- **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.
- **SMiShing** - A type of phishing attack where cell phone users receive text messages containing a website or document hyperlink; which, if clicked would lead to a malicious URL and/or download malware to the cell 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.
- **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.

What distinguishes phishing, SMiShing, and Vishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with.

Common consumer scams

Romance scams

Using fake online dating profiles with photos of other people, scammers say they are from the U.S. but are temporarily traveling or working overseas. Most romance scams start with fake profiles on online dating sites created by stealing photos and text from real accounts or elsewhere. Some of the fictitious occupations include working on an oil rig, in the military, or as a doctor with an international organization.

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 their "sweetheart" scammers money or share login credentials.

Tech support scams

Someone calls and says they're a computer technician. They might say they're from a well-known company like Microsoft or Apple, or maybe your internet service provider. They tell you there are viruses or malware on your computer, and you'll have to provide remote access to your computer or buy new software to fix it. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything.

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.

Social Security, Government & IRS scams

Scammers impersonating Social Security Administration employees over the phone to request personal information or money. Imposters may threaten consumers and demand immediate payment to avoid arrest or legal action. Many calls "spoof" official government numbers, such as SSA's National 800 Number, the Social Security Fraud Hotline, local Social Security field offices, or local police numbers. In addition, impostors may use legit names/phone numbers.

Similarly, calls from someone who says they're from the IRS. The caller may know the SSN. They say back taxes are owed, or involved in money laundering, drugs, etc. They threaten to lawsuit, arrest / deport, or revoke the SSN or license if payment is not made immediately. In order to avoid legal action, they ask for account info or are asked to send money in the form of gift cards, wire transfer or cash.

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.

Relief scams

Scammers attempt to take advantage of times of uncertainty to con people into giving up their money to aid those in need in fraudulent relief funds. Recent scams that have been attempted: flood / disaster relief; Covid-19; Ukrainian assistance; student loan debt forgiveness; and other charity scams.

Don't fall victim

Mail theft & check fraud

Mail theft and armed robberies against U.S. Postal Service carriers have increased substantially throughout the country. The criminal's focus is to gain access to the master keys of the blue USPS mailboxes – ultimately in search for checks that can be altered, counterfeited, or sold online.

In several cases, member-issued checks have been stolen from USPS mailboxes, as well as from members' mailboxes.

After stealing checks, fraudsters:

- Alter the payee and dollar amount.
- Manufacture fraudulent checks.
- Use the checks to open fraudulent new accounts and/or apply for loans using the accountholder identities listed on the checks (e.g., name and address information).

Consider these steps to help yourself

- Mail checks inside the Post Office lobby rather than using blue mailboxes.
- Pay bills online or use the credit union's bill paying service.
- Log into credit union accounts frequently to review their transaction history – looking for unfamiliar transactions.
- Report unfamiliar and unauthorized transactions immediately to the credit union.

Person-to-person (P2P) payment fraud

Fraudsters send texts to members appearing to come from the credit union warning members of suspicious transactions on their accounts through Zelle or other P2P payment option.

Nearly 18 million Americans were defrauded through scams involving digital wallets and person-to-person payment apps in 2020.

Source: The New York Times, Javelin Strategy & Research

The fraudsters call the members who respond to the texts - spoofing the credit union's phone number - and claim to be from the credit union's fraud department. The fraudster tells the member they are calling to discuss the suspicious transactions but must first verify the member's identity and ask for the member's online banking username. The fraudster then tells the member that he or she will receive a passcode and the member must provide it over the phone to the fraudster.

The fraudster initiates a transaction, such as the forgot password feature, that triggers the passcode to the member. Upon receiving the passcode from the member, the fraudster uses it to reset the member's online banking password, allowing the fraudster to login to the member's account, and use Zelle/P2P to transfer funds.

In another variation, fraudsters attempt to con members into transferring funds via Zelle to themselves using the members' own mobile phone number under the guise that it will replace funds stolen from their account; however, the fraudsters receive the transfers.

Don't fall victim

Fraudulent instruction

Fraudulent instruction wire scams involve a fraudster looking to trick a member, credit union employee, or even a title company or closing agent. The scam is usually conducted via email with fraudulent instructions to wire funds for a real estate transaction to the fraudster at the last minute.

How the real estate fraudulent wire scam works:

- A fraudster hacks into a title company or lender's email server or computer system to search for upcoming real estate closings.
- Shortly before a loan closing, fraudsters posing as the title company/closing agent send spoofed emails to credit union/ lenders or member/purchasers containing "updated wire instructions."
- Common email subject lines are:
  - Our Wiring Instructions Have Been Updated
  - We Have Sent You the Wrong Wiring Instructions
- These "updated wire instructions" are bogus and are intended to have funds sent to an account under the fraudsters' control.
- The email recipient follows the fraudulent instructions and wires the funds to the fraudster. Loss impact for these have been in the millions!

Account takeover fraud

Fraudsters also appreciate the online channel as an easier way to commit new account and account takeover fraud while concealing their true identity. Fraudsters often use consumers' personally identifiable information (PII) that is compromised in data breaches.

Losses from account takeovers through online banking have escalated over the last few years. Fraudsters have deployed sophisticated social engineering tactics allowing them to access member accounts through online banking.

Fraudsters also deploy a number of tactics to gain access to member accounts:

- Fraudsters social engineer call center employees into resetting member passwords and changing members' phone numbers used for callback verifications. They may also request changes to member email addresses and mobile phone numbers in order to intercept 2-factor authentication passcodes.
- Fraudsters social engineer members into providing login credentials.
- Fraudsters social engineer mobile carriers to intercept 2-factor authentication passcodes. Fraudsters social engineer the member's mobile carrier into activating a replacement SIM card in the fraudster's possession or porting a member's mobile service to a different carrier using the same phone number.
- Fraudsters have launched phishing and SMiShing attacks on members. The fraudulent messages appear to come from the credit union and contain links to a spoofed website designed to mimic the credit union's website where members are asked to enter their login credentials.

Don't fall victim

Text messages & spoofed websites

Fraudulent text messages - appearing to come from the credit union – containing links to spoofed websites are being sent to members. The spoofed websites are made to look like the credit unions' legitimate websites and members are enticed to click on the link and share confidential information such as username, passwords, as well as 2-factor authentication passcodes. These fraud attempts have resulted in losses from account takeovers.

The text messages have the following themes:

Alter the payee and dollar amount.

- Member's account has been locked or suspended due to suspicious or fraudulent transactions.
- Unusual/suspicious transactions at Walmart.
- Unusual/suspicious transactions at cryptocurrency exchanges.
- Suspicious Zelle transfer.

Members are instructed to click on the link contained in the message which takes the members to spoofed credit union websites where they are instructed to enter their login credentials – usernames and passwords. The fraudsters immediately use the credentials to login to the member's accounts.

Once logged into the members' accounts, the fraudsters change the member's contact information and then remove funds using Zelle/P2P or ACH transfers.

Elder abuse & financial exploitation

Elder abuse in the form of financial exploitation is at an all-time high and will continue to grow as this population category continues to grow daily.

Tech support fraud where scammers trick elderly victims into providing remote access to their computers is the most reported fraud among over 60 victims.

Other scams used against seniors include:

Elderly member scam

An elderly member receives a call from someone pretending to be their grandchild (the perpetrator may or may not know the grandchild's name). The "grandchild" indicates they have been arrested, and they need money to make bond. Circumstances, may vary or be embellished such as they have unpaid tickets they must pay before being released, or they are calling the grandparent because they don't want their parents to know.

The "grandchild" requests an amount of money needed and provides wire instructions which includes an account number of where to send the funds. The grandparent contacts the credit union and requests the wire transfer. The funds are then wired to an account controlled by the fraudster.

Contact center scam

A fraudster calls the credit union pretending to be an elderly member with a request for a new debit card since they lost the previous card. The fraudster looks to defeat weak authentication based upon known key information that a relative or someone with a legitimate purpose for being in the victim's house (e.g., caretaker) might be aware of. By defeating authentication over the phone, the scam continues and the "replacement card" is sent to the address on file where it is captured and used to gain access to account funds.

Don't fall victim

Gas pump fraud

Gas pumps are notorious for fraudsters placing skimming or shimming devices where you insert your card to capture or steal credit and debit card data.

- Inspect the card reader – check to see if anything is loose or missing.
- Check for security tape over the access door to the pump; if this is missing opt for paying inside or pick another pump
- Conceal or cover the keypad when entering your zip code and/or PIN
- Choose gas pumps which are closest to the station or retail store rather than those that are out-of-sight or in areas with little traffic
- Consider using your digital wallet applications to perform the transaction.
- Use your mobile phone to detect and monitor suspicious Bluetooth signals from potential skimmers.

Looking for additional insights?

Check out the TruStage™ risk overview: protect your identity & money for common warning signs and mitigation tips geared for credit union members.

ATM fraud

ATMs have also been targeted with hard-to-detect skimmers, keypads, and cameras to steal card and PIN information.

- Be aware of your surroundings. If you sense suspicious persons or circumstances, you most likely want to choose a different machine. Have your ATM card ready and in your hand as you approach the ATM
- Visually inspect the ATM for possible skimming devices. Potential indicators can include:
  - Sticky residue or evidence of an adhesive used by criminals to affix the device
  - Scratches
  - Damaged or crooked pieces
  - Loose or extra attachments on the card slot
  - Noticeable resistance when pressing the keypad
- Cover the pin entry pad when entering your pin. Use your other hand to shield the ATM keyboard
- Take your receipts or transaction records with you following your transaction
- Avoid visually displaying money received from the ATM and immediately put your money away
- Keep vehicle doors locked and passenger windows rolled up when using a drive-up ATM

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. TruStageTM is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.

10008618-0623 © TruStage

TruStage™