TruStage™

Don’t fall victim

Consumer fraud & scams

Each year, crafty fraudsters find different ways – email, text, phone, and even in-person - to trick consumers out of money. Of the 2.6 million fraud reports, 38% indicated money was lost – in fact, a total of $12.8 billion according to the Federal Trade Commission[1].

These fraudsters are experts in disguise which is likely why imposter scams are on the rise. They take advantage of consumer trust and introduce the sense of urgency by posing as family members, loved ones, potential romances, financial institutions, law enforcement, among others looking for victims that willingly send money, click on links, or share sensitive information.

Fraudsters target the weakest link: humans

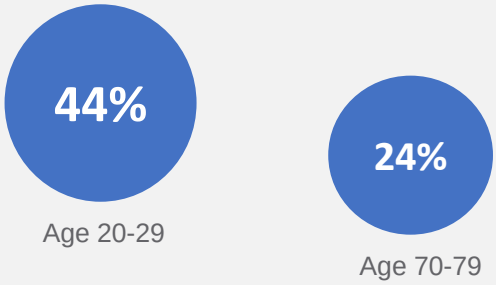
Using common channels like emails, text, and phone calls; fraudsters typically disguise their identity while retrieving confidential member information. They use tactics to succeed by tugging at the basic human instincts to trust and please. The scams look to catch your employees off-guard and/or to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

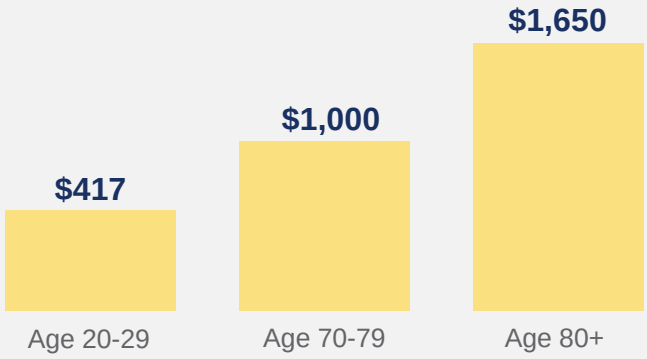
About **1 in 5 people** targeted in an imposter scam lost money according to the FTC[1]. Trending imposter scams include:

- romance
- threat of law enforcement
- government impersonation
- tech support
- investment

Younger people reported losing money to fraud **more often than older people.**



But when people aged 70+ had a loss, **the median loss was much higher.**



Source: [1]Consumer Sentinel Network Data Book 2024, Federal Trade Commission

Consumer-targeted fraud & scams

Consumer-targeted fraud continues to grow with the deceptive practices and tools criminals have access to today.

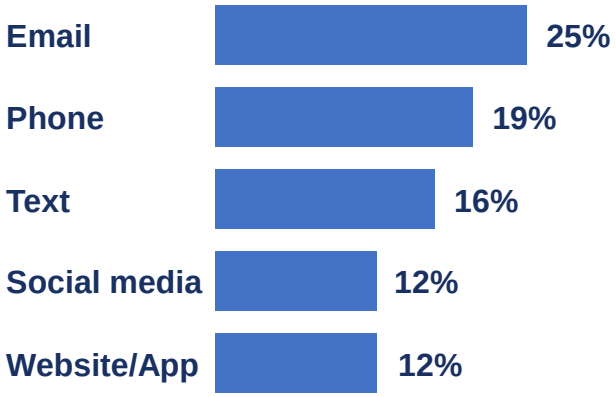
- Better and easier-to-access technology to add to the fraudster's arsenal – inflicting malware, deepfakes, and phishing campaigns
- Enhanced social engineering tactics. In addition, fraudulent business models outside of the U.S. where scammers build relationships with targets to invest – most often with crypto (aka "pig butchering")
- Breaches outside of your organizations provide fraudsters with PII and other key information
- Lack of education on the latest scams and schemes

Unfortunately, these fraudsters are getting better at tricking consumers/members into giving up money, personal information or access to accounts. Their focus is to prey on the human nature to trust, play with emotions, and introduce a sense of need or urgency. Often, consumers are recruited as money mules to assist fraudsters - knowingly or unknowingly - launder ill-gotten funds.

Consumer-targeted fraud accounts for billions of dollars lost and can erode the trust your members have in your organization.

$12.5 billion total fraud losses reported in 2024 according to the FTC[1].

Fraud reports by contact method



Source: [1]Consumer Sentinel Network Data Book 2024, Federal Trade Commission

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** attempts to acquire sensitive information via email 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** is 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** or 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.
- **Quishing** (phishing with a QR code) has become more widespread - even the US Postal Service is reporting criminals incorporating QR codes into package delivery scams. Quishing uses a QR code to redirect individuals to a fake, spoofed, or malicious website once you scan it. Scammers typically post physical images of QR codes in a high traffic locations (e.g., parking meters, public signs, event tickets, restaurants) or send them via email, text messages, and even traditional snail mail.

Common consumer-targeted fraud & scams

Typical fraudster approach

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

Fraudsters 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 and/or debit cards
- Set-up audio response or online banking

Imposter scams

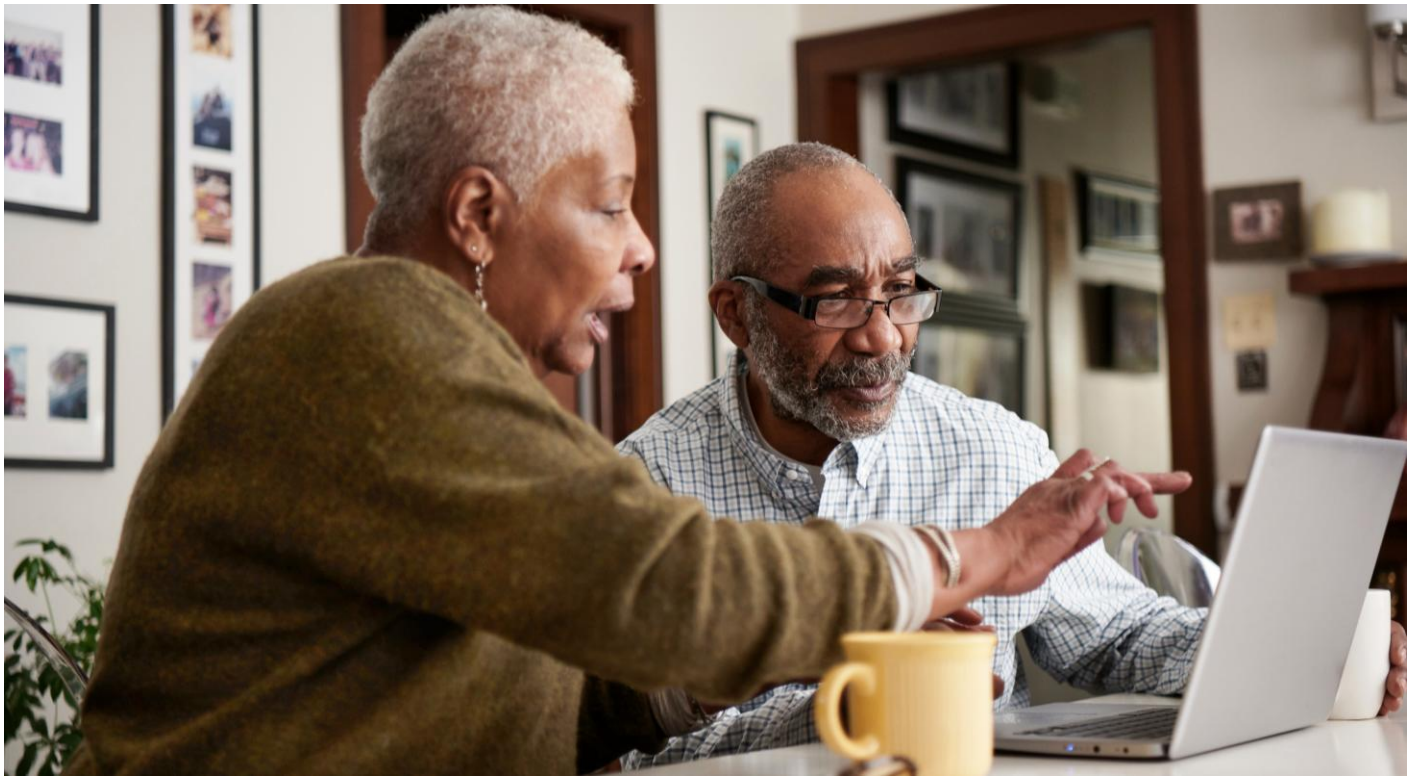
About **1 in 5 people lost money**

Source: [1]Consumer Sentinel Network Data Book 2024, Federal Trade Commission

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 call center rep into granting access to a member account than it is to hack IT infrastructure backed by a dedicated security team.

Deepfakes are also paving the way for identity theft and scams on an unprecedented scale. Fraudsters use artificial intelligence (AI) and other deepfake technologies to convincingly make it appear an individual is saying or doing something that they didn't. They create fake guises, voices and videos to successfully bypass security and controls.

Criminals also use generative AI tools and deepfake technology to produce fake identity documents — such as driver's licenses, passport cards and books — to impersonate members or open fraudulent accounts.



Common consumer-targeted fraud & scams

Mail & delivery scams
With a lot of packages being sent, shippers provide updates on the orders and deliveries. Knowing this, scammers will send phishing emails pretending to be from companies like the USPS, FedEx and UPS to lure their targets to phony webpages and get them to share personal information.

Shopping scams
Lots of shopping deals are launched – many on social media – but not all are as legitimate as they seem. It's easy to hit the "buy or submit" button on the phone or laptop but it is critical for consumers to carefully read reviews, look for security credentials on websites, and research unfamiliar retailers before taking an advantage of a discount.

Charity & investment scams
Scammers attempt to take advantage of times of uncertainty to con people into giving up their money to aid those in need – like disaster relief and other charity scams.

Investment scams
Fraudulent schemes that trick individuals into putting money into fake opportunities with false promises of high, guaranteed returns and little to no risk. Fraudsters use sophisticated tactics, including leveraging social media and AI, to gain trust and steal funds, ultimately leaving victims with significant financial losses.

Tech support scams
Someone calls and says they're a computer technician – maybe from a well-known company like Microsoft or Apple, or your internet service provider. They tell the targeted individual that there are viruses or malware on their computer, and it is necessary to provide remote computer access or buy new software to fix it. These scammers might sell your members useless services, steal card or account numbers, or get access to a computer to install malware, which could let them see everything.

Imposter scams
Fraudsters take advantage of trust between family, loved ones, potential romances, or the threat of law enforcement. Most imposter scams start with fake profiles created by stealing real photos and content. Some of the fictitious occupations include working on an oil rig, in the military, or as a doctor with an international organization.

Romance scams
Most romance scams also begin with fake online dating profiles created with stolen photos and content from real accounts. Some fictitious occupations often connect with overseas work.

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.

Social Security, Government & IRS scams
Scammers impersonating Social Security Administration employees request personal information or money. Imposters may threaten 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 and may have the victim's SSN. They say back taxes are owed, or the victim is involved in money laundering, drugs, etc. They threaten to lawsuit, arrest/deport, or revoke the SSN or license if payment is not made immediately. 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.

Advanced fee scams
The scammer informs a victim that they won a large award, lottery or is entitled to a large inheritance. However, before the victim can receive the money, they must supposedly pay taxes or fees. The victim wires funds to the scammer to pay the taxes or fees but never hears from the scammer again.

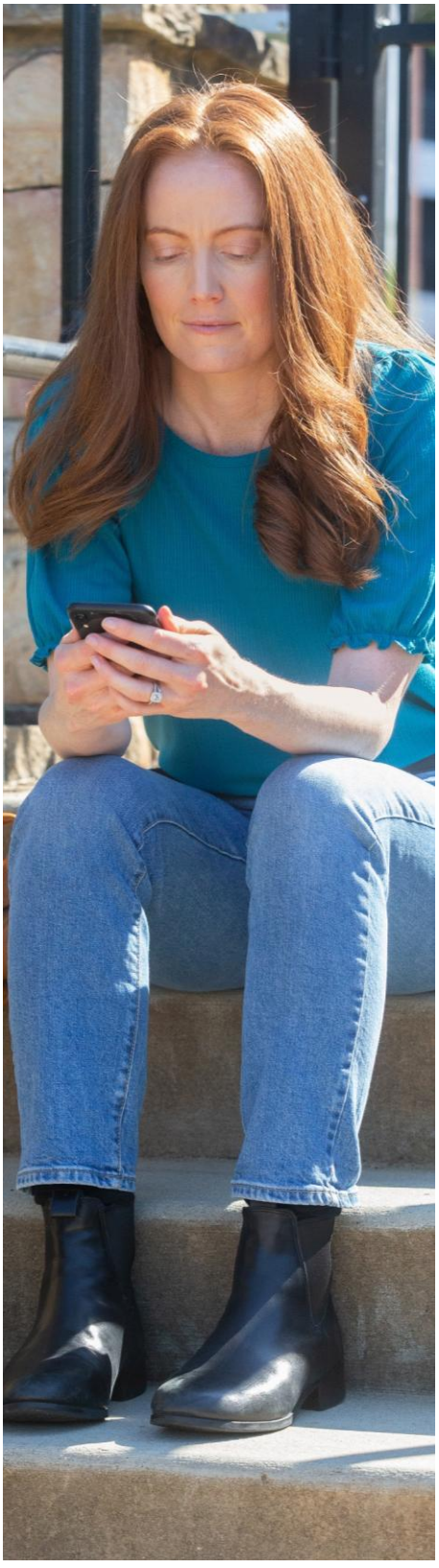
Secret shopper scams
Consumers looking to earn cash are tricked into participating in the secret shopper scam. When the consumer accepts the job, they receive a counterfeit cashier's check and are instructed to cash the check and purchase money orders and gift cards and send them to the scammers. For their efforts they can keep a percentage of the check they receive. The counterfeit check is subsequently returned unpaid and charged back to the member's account.

Common consumer-targeted fraud & scams

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

Encourage employees and members to follow these tips:

- Don't always trust the name - fraudsters will spoof the email name, phone numbers, and web page URLs to appear to be legitimate
- Check for misspelled words, bad grammar, and/or typos
- Be cautious of clicking links and opening attachments – Don't click unless you are confident of the sender or are expecting the attachment
- Do not provide personal or account information when asked. Openly sharing information on social media can provide the necessary information to impersonate you or answer some challenge questions
- Do not share a one-time passcode sent via text or email to your device(s)
- Check email salutations - many legitimate businesses will use a personal salutation
- Be suspicious of "urgent" or "immediate" response needed or "unauthorized login attempt" of your account
- Know the IRS or Social Security Administration will not contact you by phone, email, text or social media
- Don't believe everything you see. Brand logos, names and addresses may appear legitimate
- Be suspicious of random or unusual groups of people (e.g., all last names begin with same letter) on the to/recipient list
- Watch for emails or texts that appear to be a reply to a message that you didn't actually send
- Monitor the sender's email address for suspicious URLs & domains – using similar letters and numbers
- If something seems suspicious; contact that source with a new email or phone call, rather than just responding or replying directly to the email, text, or call
- Be wary of offers that appear too good to be true, require fast action, or instill a sense of fear
- Keep social media accounts private and be cautious who you're connecting with
- Never share anything related to your credit union account, transactional history, or identifying information in an unprotected public forum
- Understand that ATMs, ITMs, and gas pumps are also notorious for fraudsters to target with hard-to-detect skimmers, keypads, and cameras to steal card and PIN information
- Always report suspicious activity to the credit union as soon as possible.



Elder 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. The number of elderly fraud victims has risen at an alarming rate, while the loss amounts are even more staggering.

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've been arrested, and they need money. 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 requests the wire transfer, and 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, the "replacement card" is sent to the address on file where it is captured and used to gain access to account funds.

Elderly members that begin using services such as debit cards, home banking, wire transfers and P2P transactions - which were not previously used - are common red flags.

Face-to-face exploitation
An elderly member walks into the credit union with an individual they introduce as a relative or as a friend. They indicate they would like to add this person to their account as a joint owner, including being authorized to access their safe deposit box. The individual could be a legitimate relative, or someone the victim knows, since the exploitation is often perpetrated by a known individual.

Once the fraudster is added to the account, they can access account funds in various transactions (e.g., wires, withdrawals, P2P). Additionally, by gaining safe deposit box access, individuals can get cash, jewelry, wills, and other important documents. In some instances, older adults have lost their complete nest egg.

147,127 complaints
filed by individuals 60+

$4.885 billion
losses reported by individuals 60+

$83,000 average loss
reported by individuals 60+

Source: FBI Internet Crime Report 2024, Internet Crime Complaint Center (IC3)

Elder financial exploitation can destroy the financial security of an older adult at a vulnerable stage of life in addition to negatively impacting physical and emotional health.

Several reasons are attributed to why elder financial abuse or exploitation continues:

- Increased technology and social media use by older Americans makes seniors more vulnerable to scams
- Many seniors still have landline numbers listed in phone books, making them an easier target for telephone scammers
- Many seniors are baby boomers, and they control a vast amount of wealth that is targeted by fraudsters
- The aging population becomes more dependent on caregivers that have more day-to-day interactions
- Older adults can be more susceptive due to social isolation and mental impairment such as dementia.

Many cases of elder financial abuse can also involve family members or caregivers.

Elder financial exploitation

Frontline or account staff may know more about members based on previous conversations regarding transactions, family, work, and outside interests. This familiarity often places employees in good position to detect and protect elderly members from financial exploitation.

The key to spotting financial abuse is typically related to a change in a person's established financial patterns.

Watch out for these **red flags** during in-person, drive-up, phone, and online transactions:

- Unusual activity in a member account such as large, frequent, or unauthorized withdrawals
- A "new friend" or "family member" who accompanies the member and appears to be instructing the member to make financial decisions
- An elderly member asking to add a "new friend" or "family member" to their account
- Use of a typically inactive debit/ATM card being used for the first time, or other services previously not used such as funds transfer, online banking (bill pay), peer-to-peer transactions, etc.
- Request to increase card limits or more signs pointing to unpaid bills or late loan payments
- Closing certificate of deposits or accounts without regard to penalties
- Suspicious signatures on checks or other financial documents, or outright forgery
- New powers of attorney and/or abrupt changes in a will or other financial documents

Information can also be gathered by simply **asking questions**. Always pose questions in a way that puts the member at ease, ensure they are physically okay, and to determine if they're being exploited.

- Did you recently make a large withdrawal from your account?
- There appears to be a recent account change. Do you mind if I go over the change with you?
- We noticed an increase in the use of your debit card (or online banking). Do you mind if we review the transactions to ensure they were completed by you?
- We noticed an increase in the checks written on your account. Do you mind if we review the checks to make sure they were all written by you?

Trusted contact program

Implementing a trusted contact program can assist you when a member is convinced that they are doing the right thing. The trusted contact will not have transaction capability unless they are a joint owner; however, the contact is someone to share concerns about possible financial exploitation or the account owner's capacity to manage their account.

The program should include procedures for enrolling members and a form (created with the assistance of legal counsel) which includes:

- Trusted contact(s) information
- A section outlining circumstances when the trusted contact may be contacted to disclose information about the member's account, for example:
  - To address possible financial exploitation/ fraudulent activity
  - To confirm specifics of the member's contact information, health status, or the identity of any legal guardian
- A disclosure indicating the credit union is not required to contact the trusted contact(s) but will do so at the credit union's discretion.
- A signature space for the member

An ideal time for members to designate a trusted contact(s) is at the time of account opening. For existing members, it may be at the time of any interaction with members.

Other fraud & scams

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:

- 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.

ATM, ITM, and gas pump fraud

ATMs and ITMs – as do fuel pumps - continue to be targeted in jackpotting and other fraudulent attacks. These machines are also notorious for fraudsters placing hard-to-detect skimming or shimming devices, keypads, and cameras to capture or steal credit and debit card data.

Fraudsters carefully orchestrate attacks by targeting multiple machines located at different branches or store locations within a short period of time.

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 options.

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.

Ghost tapping

A scam referred to as ghost tapping exploits the convenience of tap-to-pay credit cards and mobile wallets. With ghost tapping, a fraudster "taps" or attempts to complete a contactless (NFC) transaction using a stolen, cloned, or compromised card credential — often through a mobile wallet, wearable device, or skimming technology.

Fraudsters often use compromised card data to enroll cards into mobile wallets creating the perfect setup for ghost tapping fraud.

Victims of the scam often discover these transactions days or weeks later because initial amounts are intentionally kept small to clear security systems. Ghost tapping can result in unauthorized transactions that fall under Regulation E or Visa/Mastercard zero-liability policies, obligating the credit union to reimburse members for losses.

Other fraud & scams

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 can be in the millions.

New account & loan fraud

Fake consumers, or synthetic identities, obtain countless deposit accounts, credit card accounts, auto loans, and personal loans costing credit unions each year.

New account fraud losses are increasing through the online channel. Fraudsters who open accounts typically use stolen identities. In addition, these fraudsters make fraudulent deposits of checks or ACH debits and withdraw the funds before the items are returned unpaid to the credit union.

Losses stemming from identity theft-related loan fraud tend to be more severe in dollar amount. Once a fraudster opens an account, usually through the online channel, they immediately apply for loans including unsecured loans, credit cards, and vehicle loans. These losses are increasing as more loan applications take place through online channels.

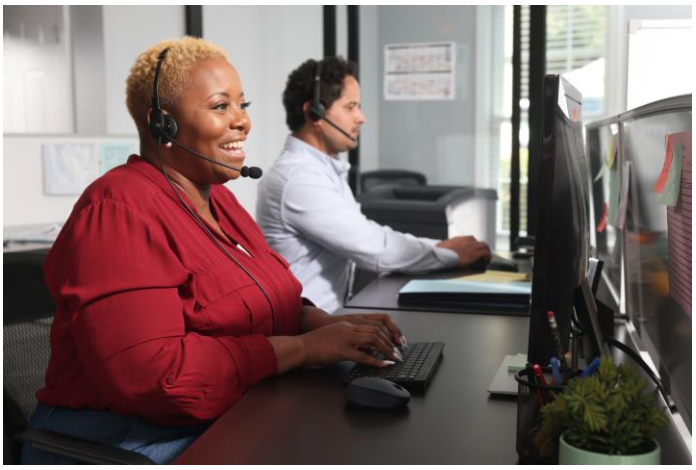
Account takeover fraud

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 will:

- deploy a number of tactics to gain access to member accounts:
- 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.
- social engineer members into providing login credentials.
- 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.
- Launch 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

How do consumers as money mules fit into scams and fraud?

Money mules are recruited by fraudsters to assist in laundering money obtained through illicit activities, such as money stolen from victims of fraud.

In many cases, fraudsters recruit money mules with bogus job offerings through online job ads or social media with promises to earn easy money for minimal work. Money mules add layers of recipients to the money trail which complicates law enforcement’s ability to track the money from the victims to the fraudsters.

Typically, money mules fall within three categories:

- **Unwitting participants** - these money mules are typically recruited through online job scams, won a sweepstakes, or strike up an online relationship and are unaware that they are engaged in criminal activity.
- **Witting participants** - these money mules are aware that they may be involved in suspicious activity but engage in it anyway.
- **Complicit participants** - these money mules are fully aware that they are engaged in criminal activity.

Money mules may open accounts under their own identity. Alternately, they may be instructed to open the accounts using a stolen or synthetic identity.

Credit unions should take proactive steps to detect suspicious/unusual transaction patterns that are indicative of money mule activity. Identifying money mule accounts starts with monitoring incoming transfers/payments to member accounts.

Knowledge gives you power to act

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.

Keep ahead of the complex array of everchanging risks, loss trends, and scams with keen awareness, effective preparation, and loss control scrutiny.

- Educate all staff on scams on an ongoing basis. Fraud and scams are often hard to detect at a quick glance; however, by being aware of common red flags, your employees can be better prepared to help and consult with members.
- Raise awareness with members by providing proactive tips and actions to ensure personal and sensitive information is not compromised. Encourage them to remain vigilant and be suspicious of unsolicited emails, texts, and calls.
- Invest in fraud detection and monitoring. Consider deploying a more secure form of two-factor authentication, such as a token or push notifications to a dedicated app residing on the member’s device. In addition, a real-time fraud monitoring solution with behavioral analytics that leverages the use of artificial intelligence and machine learning can assist in minimizing risks
- Incorporate monetary transaction limits. Ensure limits – single monetary transaction and daily limit – for all payment types offered are reasonable.
- Encourage employees access these TruStage no-cost, on-demand interactive training modules:
  - Staying ahead of check fraud
  - When members become victims

Looking for additional insights?

- Connect with a TruStage™ Risk Consultant at **riskconsultant@trustage.com** or at **800.637.2676**.
- Access the **Business Protection Resource Center** (User ID & password required) for exclusive risk resources designed to assist with your loss control efforts.

TruStage™