CUNA MUTUAL GROUP

Common Member Scams

In 2020, consumers reported losing more than $3.3 billion to fraud.

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, the Social Security Administration 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.

Of the nearly 2.2 million fraud reports, 34% indicated money was lost. In 2020, people reported losing more than $3.3 billion to fraud – an increase of nearly $1.5 billion over 2019. Using common channels like emails, text, and phone calls; fraudsters typically disguise their identify while retrieving confidential member information.

Bank transfers and payments accounted for the highest aggregate losses reported in 2020 ($314 million) with wire transfer close by ($311 million), while credit cards most frequently identified as the payment method in fraud reports.

While it can be difficult to prevent scams from happening; you can help educate your members on what to look.

Common Member Scams

- **Romance** - Scammers create fake online dating profiles to lure victims into giving them money.
- **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 Abuse** - Seniors are tricked into sending money to help their relatives / grandkids or pay for services.
- **Social Security / IRS / Government** - Threaten to suspend your social security number or arrest you or take other legal action.
- **Tech Support** – Posing as a computer technician attempts to sell services, steal PII, or get access to your computer to install malware.

FRAUD Reported

2.2 million

FINANCIAL LOSS

34% reported

Younger people reported losing money (44% age 20-29) to fraud more often than older people; however, people aged 70+ had a median loss which was much higher.

Source: Consumer Sentinel Network Data Book 2020, Federal Trade Commission

31%	Phone Call
27%	Text
15%	Email
11%	Website or Apps
6%	Social Media

% of Fraud Reports by Contact Method

Source: Consumer Sentinel Network Data Book 2020, Federal Trade Commission

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. 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.

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 romance scams 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, money mules are often used 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.

Online dating and social media have made it easier than ever to meet new people and find dates. Unfortunately, it has made scammers' work simpler, too. Con artists create compelling backstories, and full-fledged identities, then trick you into falling for someone who doesn't even exist.

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 in distress. They will often 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.

Review Elder Financial Abuse Risk Overview for additional insights and risk mitigation tips.

Social Security / IRS / Government Scams

The Social Security Administration and Office of the Inspector General continue to receive reports of scammers impersonating SSA employees over the phone to request personal information or money. Imposters may threaten you and demand immediate payment to avoid arrest or legal action. Many scam 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 legitimate names and phone numbers of SSA employees.

Similarly, you can get a call from someone who says they're from the IRS. Additionally, the caller may know some of your SSN. They say that you owe back taxes, or you're involved in money laundering, drugs, etc. They threaten to sue you, arrest / deport you, or revoke your SSN or license if you don't pay right away. In order to avoid legal action, you asked for your account info or asked to send money in the form of gift cards, wire transfer or cash.

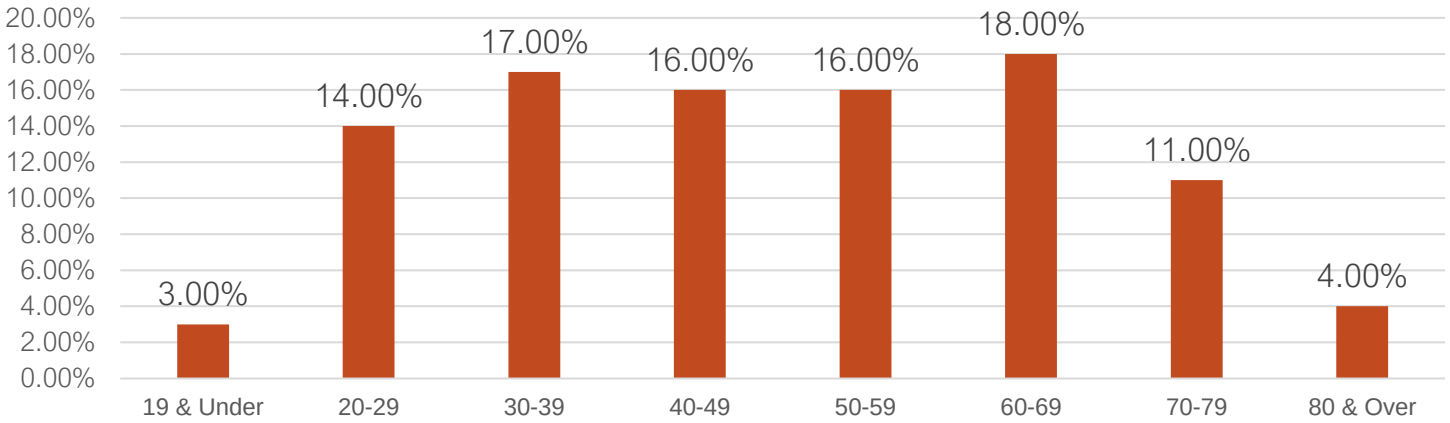
SSNs should be closely guarded – it doesn't change which makes it the ultimate prize for an identity thief.

Tech Support Scams

Someone calls and says he's a computer technician. He might say he's from a well-known company like Microsoft or Apple, or maybe your internet service provider. He tells you there are viruses or other malware on your computer. He says you'll have to give him 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 on your computer.

A common best practice is to frequently educate your employees and members about these scams. Share scams happening in your area and warning signs to help them detect and report this fraud. Check out the Federal Trade Commission Consumer Information on avoiding and reporting scams.

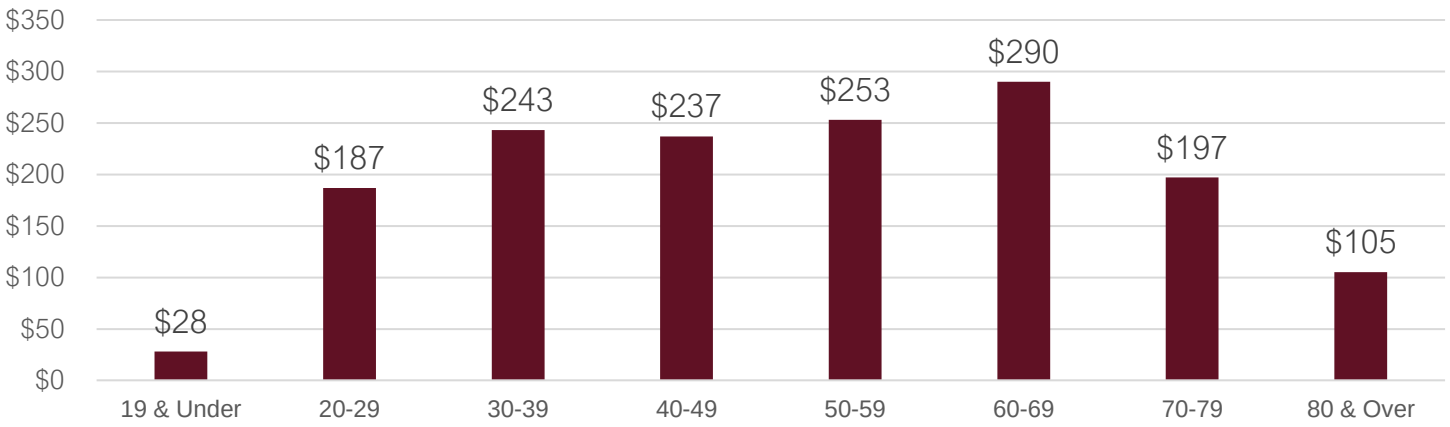
Reported Fraud by Age



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. 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 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. Warn members that if they receive these types of texts to call the institution at a phone 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 phone number of record, not a callback of the incoming number, to verify legitimacy.

Reported Losses ($s in Millions) by Age



Source: Consumer Sentinel Network Data Book 2020, Federal Trade Commission

Scam Red Flags & Prevention Tips

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.

- Don't always trust the display name - criminals will spoof the email name to appear to be a legitimate sender
- Check for misspelled words, bad grammar, and/or typos within the content
- Be cautious of clicking links and opening attachments – Don't click unless you are confident of the sender or expecting the attachment
- Do not provide personal or account information when asked. Openly sharing information on social media can provide an identity thief with the necessary information to impersonate you or answer certain challenge questions.
- Do not share a one-time passcode sent via text or email to your device
- 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 that the IRS or Social Security Administration will never 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 if the recipient group seems random or unusual (e.g., all last names begin with the same letter)
- 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 – often using similar letters and numbers
- If something seems suspicious; contact that source with a new email or phone call, rather than just hitting reply
- 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 unprotected public forums.

In October 2020, the FTC launched ReportFraud.ftc.gov, a site for people to report fraud and other illegal business practices. Reports from consumers are stored in the **Consumer Sentinel Network**, a secure online database available only to law enforcement to spot trends, identify questionable practices and targets, and enforce the law. Consumers can report as much or as little detail as they wish when they file a report.

If you'd like to learn more about member scams and scam trends,
simply schedule a no-cost personalized discussion with a CUNA Mutual Group Risk Consultant.

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