RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type | Awareness | **Watch** | Warning

Scams Target Older Americans at an Alarming Rate

The number of elderly victims impacted by fraud has risen at an alarming rate, while the loss amounts are even more staggering. In 2021, over 92,000 victims over the age of 60 reported losses of $1.7 billion to the IC3. This represents a 74% increase in losses over 2020. Many of these member-targeted scams involve fraudulent wire transfers reaching hundreds of thousands of dollars, specifically targeting your elderly members.

Every May is the nation's observance of **Older Americans Month.** This is a good time to share these scams and mitigation tips to help your credit union, employees, and members better detect and shut down attempts of financial exploitation of the elderly.

Details

The issue of elder financial abuse is likely to continue to grow as an average of 10,000 Americans turn 65 a day, a pace expected to continue through 2030 when all baby boomers will be older than 65, according to the U.S. Census Bureau.

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

- increased social media use by older Americans
- 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

Tech Support Fraud is the most reported fraud among over 60 victims with 13,900 complaints from elderly victims who experienced almost $238 million in losses.

Tech support scammers continue to impersonate well-known tech companies, offering to fix non-existent technology issues or renewing fraudulent software or security subscriptions. However, in 2021, an increase in complaints reporting the impersonation of customer support, which has taken on a variety of forms, such as financial and banking institutions, utility companies, or virtual currency exchanges.

Many victims report being directed to make wire transfers to overseas accounts, purchase large amounts of prepaid cards, or mail large amounts of cash via overnight or express services.

A recent credit union loss trend has tech support fraudsters telling victims that their identity has been stolen resulting in unauthorized withdrawals from the victim's credit union account. Several elderly members have fallen victim to this scam with one member losing over $600k when she wired funds as instructed. The fraudsters told the member there were unauthorized account withdrawals and that she needed to wire the funds from her credit union account to a protected investment account.

Date: May 17, 2022

Risk Category: Scams; Fraud; Elder Abuse; Financial Exploitation; Older Americans; Wire Transfer

States: All

Share with:

- ☐ Executive Management
- ☐ Front-line Staff / Tellers
- ☐ Human Resources
- ☐ Marketing
- ☐ Member Services / New Accounts
- ☐ People Leaders
- ☐ Risk Manager
- ☐ Transaction Services

Facing risk challenges?

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.

Scams Target Older Americans at an Alarming Rate

Another recent **sophisticated elder abuse case**, an elderly member was contacted by a fraudster posing as a bank employee (Bank A) where the member held an account. The fraudster told the member that her account at Bank A, as well as accounts the member had at other institutions including her account at a credit union, had been compromised.

This was a sophisticated scam that involved multiple fraudsters contacting the member, including one posing as an FBI agent. The fraudsters convinced the member that in order to protect her money, she needed to wire funds from her accounts at other institutions, including her credit union account, to her bank account and that the member must keep this as a secret while the FBI investigated the case.

The member was instructed to wire funds from her accounts at other institutions to her credit union account. She was then instructed to wire funds from her credit union to a third-party, which turned out to be a digital asset firm to purchase cryptocurrency.

This elderly member recently filed a lawsuit against the credit union in an attempt to recover the funds. The member alleged the credit union violated the state's elder abuse laws, including the failure to train employees to recognize signs of potential financial abuse of the elderly, and the failure to report the abuse to the appropriate state agency.

Risk Mitigation

Elder financial abuse is a growing issue for credit unions and while there is legislation to protect the elderly, credit union employees are often in the position to detect and protect their elderly members from financial exploitation. New federal and state laws prompt FIs to take an active role in trying to address fraud and scams that target older members.

Credit unions should share these important mitigation tips with their members:

- Never give control of your computer to anyone who contacts you. If you receive a call about a computer problem, hang up. If you suspect something is wrong with your computer or believe the scammer obtained access to it, bring it to a reputable company for a malware check.
- Don't trust phone numbers provided in an email, voicemail, or popup ad. If you want to call the company, use the customer service number on their official website.
- If you are asked to wire money from a recent deposit or overpayment, discuss the situation with a banker, trusted friend, or family member. Be truthful about the situation since many scammers direct you to lie about why you're sending money.

Credit unions should consider these risk mitigation tips to help protect your members from falling victim to various scams:

- Research your state's elder abuse laws and the Senior Safe Act to determine the credit union's responsibilities in helping to protect elderly members from scams.
- Develop a written, board-approved policy addressing elderly financial exploitation.
- Educate your employees and members about these scams and common red flags of financial exploitation. Share scams happening in your area and warning signs to help them detect and report this fraud.
- If the member doesn't have a history of wiring funds, consider this a red flag. Always ask your member the purpose of the wire transfer. If it appears that the member is being scammed, staff should counsel the member on the scam so that the member withdraws the request.
- Consider refusing the wire request if you suspect the member is being scammed but the member still wants to proceed with the wire.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

- Elder Financial Abuse Risk Overview
- Fraud & Scams eBook
- Member Tips: Protecting Your Identity & Money
- FBI Public Service Announcement: Technical / Customer Support Fraud

© CUNA Mutual Group, 2022

Insurance products offered to credit unions are underwritten by CUMIS Insurance Society, Inc., a member of the CUNA Mutual Group. This RISK Alert is intended solely for CUNA Mutual Group Fidelity Bond policyowners to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

This resource was created by CUNA Mutual Group based on our experience in the credit union, insurance, and risk management marketplace. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value, and implementing loss prevention techniques. No coverage is provided by this resource, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.