RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Scammers Continue To Take Advantage of Lonely Hearts

Millions of people, including credit union members, look to online dating or social networking sites to meet someone. But instead of romance, many unknowingly find a scammer. Cyberspace scammers are eager to take advantage of lonely hearts by setting up fake accounts on social media or dating sites to establish fraudulent relationships and get them to send money. In fact, the median loss of romance / sweetheart scams as reported by the Federal Trade Commission (FTC) is $2,600 and for people over 70 was over $10,000.

Details

Scammers continue to fake online dating profiles using photos or other people to lure their victims. People reported losing $143 million to romance and sweetheart scams according to the FTC. The scammers strike up a relationship with their targets to build their trust, sometimes talking or chatting several times a day. The scammers quickly profess their love and tug at the victim's emotions with fake stories and their need for money.

By using popular social media sites - like Instagram, Facebook, or Google Hangouts - scammers make the connection quickly and con their victims into wiring money or sending gift cards from vendors like Amazon.

Another variation is where victims are duped into providing online banking login credentials. The scammer then logs into the account and uses the account-to-account / external transfer feature to initiate ACH debits against accounts at other institutions pulling funds into the victim's account for deposit, or deposit fraudulent checks via mobile remote deposit capture. 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, and checks are returned unpaid.

A few red flags of these romance / sweetheart scams:

- String you along but never want to meet in person
- Scammers often say they're living / traveling outside of the United States
- Hint they're having money trouble and ask for money, personal info, or account number
- Often need money for emergencies, hospital bills, or travel.

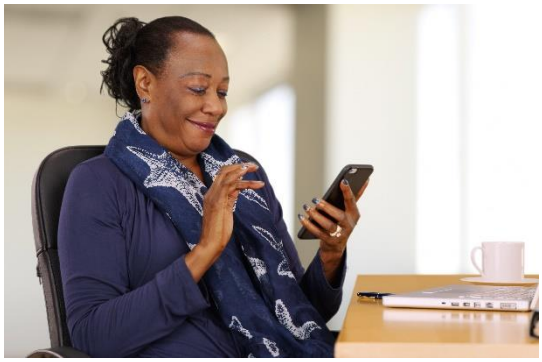
Date: January 23, 2020

Risk Category: Consumer Payments, Fraud, Scams, Cybersecurity

States: All

Share with:

- ☐ Executive Management
- ☐ Front-Line Staff / Tellers
- ☐ Marketing
- ☐ Member Services / New Accounts
- ☐ Plastic Cards Department
- ☐ Risk Manager



Your feedback matters!

Was this RISK Alert helpful?

Vote Yes | Vote No

Scammers Continue To Take Advantage of Lonely Hearts

Risk Mitigation

Educate your staff and members with these tips:

- Provide warnings to your members on this scam through your newsletter and/or by posting articles on your website. Encourage your members to review their accounts daily and report any discrepancies immediately.
- Encourage members to slow down and talk to someone they trust – don't let a scammer rush or bully them into something.
- Never send money or gifts to a sweetheart you haven't met in person - never wire money, put money on a gift or cash reload card, or send cash to an online love interest.
- If your member thinks it is a scam, report it to the FTC at ftc.gov/complaint. Be sure to notify the website or app where you met the scammer, too.

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.

Review these specific resources for more information

- Common Member Scams
- Elder Financial Abuse Risk Overview
- Protect Yourself – Member Protection Tips
- The Rise of Social Engineering Fraud

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for white papers & checklists
- Webinars and Education
- RISK Alerts Library

Check out these areas of practice to help you manage pressing risks.

The Protection Resource Center requires a User ID and Password.

Interested in learning more about fraud, scams, and other emerging risks?

Contact CUNA Mutual Group's Risk & Compliance Solutions at **800.637.2676** or riskconsultant@cunamutual.com