Members Romanced Into Providing Login Credentials and Money

Romance and dating scams continue to victimize credit union members nationwide. Fraudsters ultimately convince them to provide account login credentials. These scammers then login to the account and use ACH debits or enroll for mobile remote deposit capture to deposit fraudulent checks. The members subsequently transfer the funds to the scammer before the ACH debits or checks are returned.

Details

Scammers continue to fake online dating profiles using photos or other people to lure their victims. Once connected, the scammers often say they are from the U.S., but are temporarily traveling or working overseas. The scammers quickly profess their love and tug at the victim’s emotions with fake stories and their need for money. The victims often send the scammers money or provide online banking login credentials.

In fact, more than 12,500 complaints related to the romance scam with losses totaling $203 million were reported in 2015, according to the FBI.

Other romance scam variations include:

- Victims are duped into providing online banking login credentials to the scammers under the guise the scammers do not have access to financial services in the foreign country in which they are traveling or working. The scammer logs into the account and uses the account-to-account (A2A) / external transfer 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.

- 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.

To share risk insights or gain additional assistance:

- Report a RISK Alert
- Ask a Risk Consultant
- Contact a CUNA Mutual Group Risk Consultant
  - 800.637.2676, option 4
  - riskconsultant@cunamutual.com
Victims are characteristically female, maintain a modest financial means and typically have few assets to cover negative account balances that result from the return of the ACH debits or checks. In most cases, credit unions end up charging off the negative account balances.

**Risk Mitigation**

Credit unions should consider these mitigation tips:

- Protect members by establishing criteria, such as creditworthiness / credit scores, to qualify members for account-to-account (A2A) / external transfer service and mobile remote deposit capture.

- Provide warnings to your members on this scam through your newsletter and/or by posting articles on your website.

- Encourage your members to follow these specific safeguards for online dating:
  - Research the person’s photo and profile using online searches to see if the material has been used elsewhere.
  - Go slow and ask lots of questions.
  - Beware if the individual seems too perfect or quickly asks you to leave a dating service or Facebook to go “offline.”
  - Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
  - Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can’t. If you haven’t met the person after a few months, for whatever reason, you have good reason to be suspicious.
  - Never send money to anyone you don’t know personally.

**Risk Prevention Resources**

Access CUNA Mutual Group’s Protection Resource Center at cunamutual.com for exclusive Risk Management resources to assist with your loss control needs. The Protection Resource Center requires a User ID and password.

- Overview: ODFI of Debits / Online Deposits
- Whitepaper: Remote Deposit Capture
- Webinar: Spam, Shams, and Other Scams (recorded April 19, 2017)

Contact a CUNA Mutual Group Risk Consultant at 800.637.2676, option 4, riskconsultant@cunamutual.com, or use Ask a Risk Consultant for additional risk insights and to learn how our team of consultants can assist your credit union.

© CUNA Mutual Group, 2017.

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.