RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Member HELOCs Used to Fund Counterfeit Checks

Credit unions have incurred large losses from counterfeit checks that draw funds from members' home equity lines of credit (HELOCs), including counterfeit HELOC checks and counterfeit checks drawn on member checking accounts funded from unauthorized advances against member HELOCs. In many cases, fraudsters social engineered call center employees to request a canceled HELOC check or to order share drafts on member accounts.

Details

HELOC-related fraud can lead to large losses and are relatively easy to execute by using stolen personally identifiable information (PII). Many cases involve fraudsters – impersonating members – social engineering call center employees into providing a copy of a canceled HELOC check. Losses from a single counterfeit HELOC check have ranged from $30,000 to $350,000.

Recorded mortgages, including HELOCs, are normally public records which allows fraudsters to search for open HELOCs. Once found, the records typically have borrower signatures and account numbers which the fraudsters capture for later use in committing fraud. For example, a fraudster may send a fax to have HELOC checks sent to a new address with the fax containing an image of the actual member's signature. Fraudsters have also counterfeited checks, as well as order checks, against member checking accounts that end up being funded by unauthorized advances against members' HELOCs.

Credit union case study:

> A fraudster social engineered a call center employee into changing a member's address and phone number. The fraudster social engineered the call center again two days later to reset the member's online banking password. This allowed the fraudster to login to the member's account to order share drafts which were delivered to the new address. The fraudster forged three share drafts totaling $407,000 and funded them through unauthorized advances against the member's HELOC through online banking.

A common occurrence with these losses has members falling victim to phishing scams that result in credential-stealing malware downloaded to their mobile device or computer system. Fraudsters login to member accounts and change addresses and phone numbers, order HELOC checks or share drafts, and take advances from HELOCs transferring the funds to checking accounts.

Date: November 10, 2020

Risk Category: HELOCs; Deposit Account Services; Lending Risks; Counterfeit Checks; Scams; Fraud

States: All

Share with:

- ☐ Collections
- ☐ Compliance
- ☐ Loan Manager
- ☐ Member Services / New Accounts
- ☐ Risk Manager

Your feedback matters!

Was this RISK Alert helpful?

Vote Yes | Vote No

Member HELOCs Used to Fund Counterfeit Checks

Risk Mitigation Tips

Credit unions should consider these mitigation tips

- Allow members to opt-out of receiving blank HELOC checks or avoid sending members unsolicited blank HELOC checks.
- Don't allow members to link overdrafts to HELOC accounts.
- Train staff to be aware of pretext calling attempts to obtain member account information, such as requests for canceled checks drawn on member HELOC accounts.
- Ensure use of a strong authentication method (e.g., identity verification service) to verify the identity of members.
- If using member identification questions, ensure the use of out-of-wallet questions that are account-specific and not found on online banking statements, within online banking sessions, or the monthly statement mailed to members.
- Information that typically represents good out-of-wallet questions include:
  - Year member's account was opened
  - Branch at which member's account was opened
  - Color of vehicle securing the member's loan
  - Last loan paid off, approximate date, and collateral used
  - Name of two non-utility payees if the member uses bill pay
  - Whether the member receives paper or e-statements
  - Payable on death beneficiary
  - List of account(s) on which the member is joint owner
- Establish formal procedures to perform a review of members' checks, including HELOC checks, presented for payment that exceeds an established monetary threshold:
  - Verify member signatures against the signature cards or other reliable documents (e.g., loan documents).
  - Verify the check characteristics against legitimate checks.
  - Contact the member to verify that they actually issued the check(s).
  - Perform a timely review allowing the credit union to return unauthorized checks by the required midnight deadline.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk resources to assist with your loss control. The Protection Resource Center requires a User ID and password. Review this resource to learn more:

- Liability for Forged Member Share Drafts Under the UCC

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.

Facing risk challenges?

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