RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Account Takeovers Stemming From Credit Card Management Systems

Credit unions utilizing credit card management systems offered by card processors have reported fraud due to account takeovers. These systems allow members to view balances and recent transactions, sign-up for and access e-statements, and make payments 24/7. Fraudsters are enrolling compromised cards for this service by exploiting weak authentication measures.

Details

Fraudsters are using social engineering tactics such as phishing, vishing and smishing to gain access to members' personal account information. Credit unions that offer members access to credit card management systems from their card processors for payments and account management of their credit union-issued credit cards have reported fraud due to account takeovers. By enrolling compromised credit cards in the card management system, fraudsters are exploiting weak authentication measures.

Account takeover fraud is a type of identity theft where fraudsters gain access to members accounts, then make non-monetary changes that may include modifying members personally identifiable information. Fraudsters use stolen identities to impersonate members by enrolling member accounts for online banking. Once enrolled, they change the member's contact info through online banking. When logged into the account, fraudsters access the credit card management system site to:

- create profiles for cardholders
- change cardholders' phone numbers
- change cardholder e-mail addresses to the fraudsters' email.
- make fraudulent payments via ACH to free up credit limit
- initiate a card transaction to receive a fraud alert to the updated mobile phone number on file and confirm the fraudulent transaction as a valid cardholder transaction

A key indicator of fraud are transactions that involve the purchase of cryptocurrency.

Risk Mitigation

Credit unions using the card processor's credit card management system for members to manage their cards should consider these risk mitigation tips:

- Avoid placing the link to the card processor's credit card management system on your public-facing website. Instead, place the link within online banking.

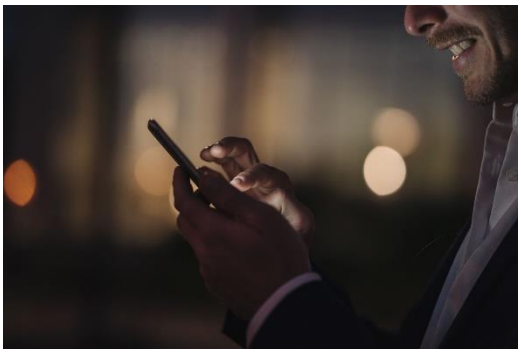
Date: December 21, 2021

Risk Category: Account Takeover; Scams; Fraud; Plastic Cards; Social Engineering;

States: All

Share with:

- ☐ Executive Management
- ☐ Member Services / New Accounts
- ☐ Plastic Cards / Cards Department
- ☐ Risk Manager
- ☐ Transaction Services



Facing risk challenges?

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

Risk Mitigation (continued)

- If cardholders are able to change their contact information through the system, card services staff should review file maintenance reports provided by your credit card processor for changes to cardholder information on file, such as changes to phone numbers and email addresses.
- Work with your card processor to evaluate the authentication measures for members who enroll for this service. Credit unions are encouraged to demand a strong authentication method to mitigate account takeover risk.
- Inform members to never provide personal information in response to a text message or phone call purportedly from the credit union.
- Advise members that no credit union employee would ever ask for personal information, such as account numbers, usernames, passwords, and passcodes.

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.

- Fraud & Scams eBook
- Two-Factor Authentication Risk Overview
- Social Engineering Fraud Risk Overview
- Member Authentication & Verification Risk Overview

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.