RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Sophisticated Social Engineering Scams Lead to P2P Fraud

Fraudsters are launching social engineering attacks to members by posing as the credit union to obtain online banking credentials. They are defeating out-of-band / 2-step authentication by scamming the member into providing this passcode to them. Once they have the passcode, they login to the member's account and use peer-to-peer (P2P) services, such as Zelle and Payzur, to transfer funds elsewhere. Credit unions have reported losses ranging from $30,000 to $2 million due to this fraudulent activity.

Details

Account takeovers have recently caused large losses for credit unions. Fraudsters are tricking members to provide their login credentials through social engineering tactics. Many of these losses involve credit unions that offer peer-to-peer payment (P2P) services like Zelle and Payzur.

Criminals are aware that credit unions are utilizing out-of-band / 2-step authentication to further authenticate a member by sending a one-time passcode to their mobile device. Fraudsters have deployed a sophisticated social engineering attack against members to obtain that passcode which they use to login to member accounts. Once they have access to online banking, the fraudsters will change contact information as well as passwords on the account.

Here's how the scam works:

Fraudsters send account alerts to members via text message – appearing to come from the credit union – warning them of suspicious debit card activity.

- For those members who respond to the text, the fraudsters call the members spoofing the credit union's phone number and claim they are in the credit union's fraud department and calling to verify suspicious transactions.
- To verify the member's identity, the fraudster explains a passcode will be sent via text message and the member must provide the passcode over the phone.
- The fraudsters attempts a transaction that triggers a 2-step authentication passcode, such as using the "forgot password" feature or initiating a P2P transaction. The passcode is sent via text / email to the member who, in turn, provides it to the fraudster.
- The fraudsters immediately use the passcode to login to the member's accounts and use the P2P feature to transfer funds.

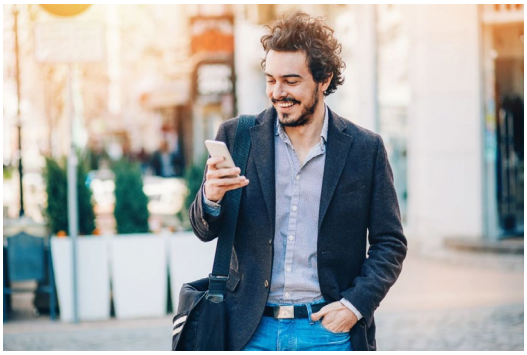
Date: May 12, 2020

Risk Category: Consumer Payments, Peer-to-Peer Payments, Fraud, Social Engineering, Plastic Card, E-Commerce

States: All

Share with:

- ☐ Call Center Staff
- ☐ Electronic Services
- ☐ Executive Management
- ☐ Plastic Cards Department
- ☐ Risk Manager
- ☐ Transaction Services



Your feedback matters!

Was this RISK Alert helpful?

Vote Yes | Vote No

Sophisticated Social Engineering Scams Lead to P2P Fraud

Fraudsters also have spoofed the credit union phone number and called members asking them to verify information such as card number, PIN and CVV/CVC – which is all they need to counterfeit a card.

In a few cases where members refused to provide the passcode, the fraudsters impersonated the members and social engineered the members' mobile phone carrier to port the members' mobile phone to a different carrier. This allows the fraudster to receive the passcode by using the "forgot password" feature.

Additionally, credit unions have reported that fraudsters successfully social engineered the credit union's call center employees into changing mobile phone numbers on member accounts, allowing the fraudsters to receive the passcodes. Fraudsters have also been known to hack member email accounts to intercept passcodes sent via email.

Risk Mitigation Tips

Consider these risk mitigation tips:

- At the first sign of fraud, disable passive enrollment for P2P by requiring members to enroll at a branch or call the credit union after properly authenticating members.
- Implement a waiting period, such as 2 days, before newly enrolled members may use P2P.
- Implement lower daily limits for new users for the first few P2P transactions to reduce the risk exposure.
- Block or delay transfers following a password change. Password changes are a common red flag of an account takeover.
- Block P2P tokens that are found to be fraudulent. A P2P token refers to the email or mobile number of the intended recipient of the transfer.
- Use a real-time fraud monitoring solution that can identify password changes using a device not recognized, immediate enrollment in P2P, and an addition of a new token.
- Include a statement in texts and emails containing the passcode, such as "If you did not request this passcode call the credit union immediately. Don't share this passcode with anyone. Credit union employees will never ask for this passcode."
- Warn members of smishing and vishing scams. Instruct members to not respond to SMS text messages or calls, even if they appear to come from the credit union. Advise members to call the credit union using a reliable phone number to question any SMS text messages or voice calls purportedly from the credit union.

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 these resources to learn more:

- Peer-to-Peer Payments Risk Overview
- The Rise of Social Engineering
- Risk Alert: Fraudsters Target Members Through Social Engineering Attacks
- Risk Alert: Large Fraud Losses Involving Peer-to-Peer Payments Reported

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.