RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

New Twist to the Zelle Fraud Scam

Fraudsters continue to target members of credit unions offering Zelle by using a sophisticated scam to defeat 2-step authentication (also referred to as out-of-band authentication), which leverages the use of one-time passcodes. In a new twist to this scam, fraudsters are defeating out-of-band authentication with transaction details, which Zelle introduced to help curb the fraud.

Details

Credit unions offering Zelle started reporting large fraud losses in 2019 as a part of a sophisticated scam targeting their members. Fraudsters continue to target members of credit unions offering Zelle by using a sophisticated scam to defeat 2-step authentication (also referred to as out-of-band authentication), which leverages the use of one-time passcodes.

Here's how the scam works:

- Fraudsters send text alerts to members – appearing to come from the credit union – warning members of suspicious debit card transactions.
- Fraudsters call those members who respond to the text - spoofing the credit union's phone number - and claim to be from the credit union's fraud department.
- To verify the identity of the member, the fraudster asks for the member's online banking username and tells them they will receive a passcode via text or email and the member must provide it to the fraudster. In reality, the fraudster initiates a transaction, such as the forgot password feature, that generates a 2-step authentication passcode which is delivered to the member.
- The member provides the passcode to the fraudster who uses it to log in to the member's account using a device not recognized by the host system.
- Upon logging into the accounts, fraudsters change the online banking passwords and then use Zelle to transfer funds to others.

Note that fraudsters prefer to target Zelle due to the speed in which the transfers are made (minutes versus hours or days); however, the fraudsters have targeted other vendor P2P products offered by credit unions.

To combat this scam, Zelle introduced out-of-band authentication with transaction details. This involves sending the member a text containing the details of a Zelle transfer - payee and dollar amount – that is initiated by the member. The member must authorize the transfer by replying to the text. Unfortunately, fraudsters are defeating this layered security control.

Date: January 19, 2021

Risk Category: Fraud; Scams; Peer-to-Peer Payments; Social Engineering; Consumer Payments; E-Commerce

States: All

Share with:

- ☐ Call Center Staff
- ☐ Electronic Services
- ☐ Member Services / New Accounts
- ☐ Risk Manager
- ☐ Transaction Services

Facing risk challenges?

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

New Twist to the Zelle Fraud Scam

The fraudsters follow the same tactics except they may keep the members on the phone after getting their username and 2-step authentication passcode to log in to the accounts. The fraudster tells the member they will receive a text containing details of a Zelle transfer and the member must authorize the transaction under the guise that it is for reversing the fraudulent debit card transaction(s). The fraudster actually enters a Zelle transfer that triggers the following text to the member which the member authorizes:

> **Send $200 Zelle payment to Boris Badenov? Reply YES to send, NO to cancel. ABC Credit Union <valid credit union phone number>. STOP to end all messages.**

Risk Mitigation

Credit unions should consider these mitigation tips:

- Educate members on this scam instructing them to be wary of texts or calls appearing to come from the credit union. Advise members to call the credit union using a reliable phone number to question any text message or phone call purportedly received from the credit union.
- Inform members to never provide personal information in response to a text message or phone call purportedly from the credit union.
- Advise members no credit union employee would ever ask for personal information, such as account numbers, usernames, passwords, and passcodes.
- Avoid sending 2-step authentication passcodes via email due to the risk of email hacking.
- Disable passive enrollment for peer-to-peer payments (P2P) and require members to enroll in person at a branch or through the call center after properly authenticating the members.
- Block or delay P2P transfers that are initiated immediately following a password change using a device not recognized by the host system. Confirm the transfers by contacting the member.
- Deploy a real-time fraud monitoring system with behavioral analytics.
- Ensure call center staff use strong out-of-wallet questions to authenticate members, particularly when members request a change to their contact information, such as mobile phone number and/or email address.

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.

- RISK Alert: Fraudsters Target Members Through Social Engineering Attacks
- Risk Overview: The Rise of Social Engineering Fraud

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.