RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Fraudsters Change Tactics in Zelle / P2P Fraud Scam

The Zelle / P2P fraud scam is widespread and has been making local and national news as the social engineering tactics used by fraudsters in this scam continue to evolve. A **newer version of the scam** has fraudsters, impersonating a Zelle user's financial institution, conning the user into using Zelle to transfer funds to themselves using their mobile phone number under the guise that it will replace funds stolen from their account. However, the Zelle transfers go to the fraudsters.

Details

The Zelle / P2P fraud scam continues to result in large fraud losses for credit unions. Fraudsters continue to target members of credit unions; however, they've adapted to a newer version of the scam that has made headlines across the country.

Here's How It Works:

- Fraudsters send text alerts to users – appearing to come from their financial institution – asking the users if they attempted a large dollar Zelle transfer.
- Fraudsters immediately call the users who respond 'NO' by spoofing the FI's phone number and claim to be from the FI's fraud department.
- Fraudsters tell the users the Zelle transfers went through, but the funds can be recovered.
- Fraudsters tell the users in order to recover the stolen funds they must use Zelle to transfer the funds to themselves using the users' mobile phone number, but before doing so, the fraudsters instruct the users to disable their mobile phone number associated with their Zelle account.

  Note: Fraudsters may have previously opened an account at the user's FI (likely using a stolen identity) and establishes Zelle through the online or mobile banking channel linking the member's mobile phone number to Zelle.
- When the fraudster links the user's mobile phone number to the fraudster's Zelle account, a 2-factor authentication passcode is generated and sent to validate the mobile phone number. The text message containing the passcode is actually sent to the user's mobile phone; however, the fraudster cons the user into providing the passcode over the phone. (The text containing the passcode has the FI's name which explains why fraudsters open a fraudulent account at the user's institution.)
- The fraudster enters the passcode to activate the mobile phone number on their Zelle account.
- Users are instructed to Zelle themselves the funds.
- The Zelle transfers actually go to the fraudsters.

Date: March 15, 2022

Risk Category: Online / Mobile Banking; Scams; P2P; Scams; Fraud

States: All

Share with:

- ☐ Executive Management
- ☐ People Leaders
- ☐ Risk Manager
- ☐ Transaction Services

Facing risk challenges?

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

Fraudsters Change Tactics in Zelle / P2P Fraud Scam

The question of whether consumers victimized in the new version of the scam are entitled to protection under Reg E appears to be a gray area based on Reg E's definition of an unauthorized electronic fund transfer (EFT).

Under §1005.2(m), an unauthorized EFT is one that is initiated by someone other than the consumer without authority to initiate the transfer and from which the consumer receives no benefit. In the new version, Zelle users initiate the transfers rather than the fraudsters. Hundreds of complaints have been filed with the CFPB by Zelle users.

We are unsure if this newer version of the Zelle fraud scam has impacted credit union members. The fraud cases reported by credit unions so far have involved fraudsters initiating the fraudulent Zelle transfers after scamming members out of their login credentials. Several credit unions were hit by scam the same month in which they introduced Zelle to the membership.

Our previously-issued RISK Alert – New Twist to the Zelle Fraud Scam – provides an overview of how the scam works.

Risk Mitigation Tips

Credit unions offering or contemplating Zelle should consider these risk mitigation tips:

- Launch Zelle with lower daily limits which helps keep initial fraud losses low. The limits can be raised at a later date.
- Require members to enroll for Zelle in person at a branch or through the call center after they are properly authenticated.
- Block/delay Zelle transfers that occur immediately following a password reset using a device not recognized by the host system so that they can be investigated.
- Deploy a real-time fraud monitoring system.
- Include a statement in texts and emails containing 2-factor authentication passcodes, 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."
- Educate members on this scam instructing them to be wary of texts or calls appearing to come from the credit union. Advise members to never use Zelle to transfer funds to themselves and to call the credit union using a reliable phone number to question any text message or phone call purportedly received from the credit union.
- If your members are impacted by the newer version of the scam where they are instructed to use Zelle to transfer funds to themselves, consult with legal counsel to determine your obligations under Reg E.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk resources, RISK Alerts, and on-demand webinars (User ID and Password required).

Check out these specific resources:

- RISK Alert Library: New Twist to the Zelle Fraud Scam
- Peer-to-Peer Payments Risk Overview
- Emerging Risks Outlook: Zelle/P2P 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.