RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Reg E & the New Version of the Zelle / P2P Fraud Scam

In the new version of the Zelle / P2P fraud scam, fraudsters con Zelle users into using Zelle to transfer funds to themselves using their mobile phone number under the guise that the transfer will replace funds stolen from the users' accounts; however, the transfers go to the fraudsters. An attorney with the Consumer Financial Protection Bureau (CFPB) has shared informal non-binding guidance on whether consumers are entitled to protection under Reg E.

This is a follow-up to the RISK Alert, Fraudsters Change Tactics in Zelle / P2P Fraud Scam.

Details

We reached out to the CFPB using its regulatory inquiries system to determine whether consumers victimized in the new version of the Zelle / P2P fraud scam are entitled to protection under Reg E. An attorney with the CFPB provided us with informal non-binding guidance.

The attorney referred to Section 2.3.1 in the CFPB's Fall 2021 Supervisory Highlights that was issued in December 2021. The attorney reasoned that the Zelle transfer initiated by the user using their own mobile phone number should be considered a "token error." A token error occurs when a Zelle user enters the recipient's "current and accurate phone number or email address," but the transfer is misdirected to an unintended recipient. Token errors are "incorrect electronic fund transfers" (EFTs), which are a defined error under §1005.11(a)(1)(iii).

The following is an excerpt from Section 2.3.1:

> Supervision conducted examinations of institutions in connection with the provision of person to-person digital payment network services. Regulation E defines the term "error" to include, among other things, "[a]n incorrect electronic fund transfer to or from the consumer's account." Regulation E requires institutions to investigate promptly and determine whether an error occurred. Examiners found that, in certain cases, due to inaccurate or outdated information in the digital payment network directory, consumers' electronic fund transfers (EFTs) were misdirected to unintended recipients, even though the consumer provided the correct identifying token information for the recipient, i.e., the recipient's current and accurate phone number or email address. These misdirected transfers are referred to as "token errors." Token errors are incorrect EFTs because the funds are not transferred to the correct account. Examiners found that institutions violated Regulation E by failing to determine that token errors constituted "incorrect" EFTs under Regulation E.

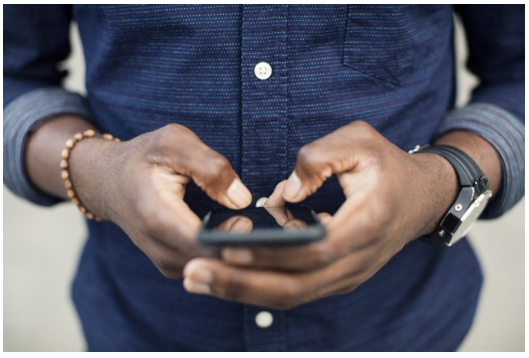
Date: May 3, 2022

Risk Category: Compliance; P2P; Fraud; Scam; Online / Mobile Banking

States: All

Share with:

- ☐ Compliance
- ☐ Executive Management
- ☐ Legal
- ☐ Risk Manager
- ☐ Transaction Services



Facing risk challenges?

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

Reg E & the New Version of the Zelle / P2P Fraud Scam

In the traditional Zelle/P2P fraud scam, members are scammed into providing their login credentials (usernames and 2-factor authentication passcodes) and/or debit card details to the fraudsters, resulting in unauthorized Zelle transfers or unauthorized debit card transactions. The CFPB's Electronic Fund Transfer FAQs clearly indicate that consumers victimized in the traditional scam are entitled to protection under Reg E. Refer to questions 4 and 5 under the category, "Error Resolution: Unauthorized EFTs."

Risk Mitigation

Based on the informal non-binding guidance provided by the CFPB, it appears that members victimized in the new version of the Zelle / P2P fraud scam are entitled to protection under Reg E. However, you may want to consult legal counsel to determine your obligations under Reg E.

Risk Prevention Resources

Access CUNA Mutual Group's **Protection Resource Center** for exclusive risk and compliance resources (User ID and Password required).

Check out these resources for more details on this scam:

- Emerging Risks Outlook: Zelle / P2P Fraud
- Peer-to-Peer Payments Risk Overview
- RISK Alert: Fraudsters Change Tactics in Zelle / P2P Fraud Scam
- RISK Alert: CFPB Issues Important FAQs on EFTs
- RISK Alert: New Twist to Zelle Fraud Scam

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.