RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Vishing Scam Leads to PIN-Based Debit Fraud

Members are being targeted in a vishing (phone-based phishing) scam in which fraudsters spoof phone numbers making the calls appear to originate from the credit union. The members are duped into providing CVV2/CVC2 codes and expiration dates for their debit cards. The fraudsters, already possessing the counterfeit mag stripe debit cards, use the information to change the PINs through voice response units. Then, they use the counterfeit cards to make ATM withdrawals, as well as purchases at Wal-Mart in Florida and Georgia. Credit unions in Indiana, Kentucky, Ohio, and Virginia have been impacted by the scam.

Details

Fraudsters targeting members through a vishing scam (phone-based phishing) are spoofing credit union phone numbers and posing as an employee in the credit union's fraud or security department. The fraudsters tell the members they are calling to verify suspicious debit card transactions and, to verify the member's identity, the member's are asked to provide the CVV2/CVC2 code and the card's expiration date.

Because the fraudster already has counterfeit debit cards on hand, they use the information obtained to change the members debit card PIN through the card processor's voice response unit (VRU).

Changing debit card PINs using the card issuer's VRU typically requires the cardholder to pass three of five security tests:

- Call must originate from cardholder's phone on file with the card issuer;
- Provide the three-digit security code on the card's signature panel (CVV2/CVC2);
- Card expiration date;
- Card holder's date of birth;
- Last four digits of the cardholder's Social Security number

Date: August 21, 2018

Risk Category: Scams; Plastic Card Fraud; Phishing; Vishing; ATMs

States: All

Share with:

- ☐ Branch Operations
- ☐ Executive Management
- ☐ Front-Line Staff / Tellers
- ☐ Plastic Cards / Cards Department
- ☐ Risk Manager

To share risk insights or gain additional assistance:

- Report a RISK Alert
- Ask a Risk Consultant
- Contact a CUNA Mutual Group Risk & Compliance Consultant
  - **800.637.2676**
  - riskconsultant@cunamutual.com

Vishing Scam Leads to PIN-Based Debit Fraud

In most cases, the fraudulent debit card transactions are coming through as fallback transactions. Fallback transactions occur when an EMV-enabled terminal (POS or ATM) cannot read the chip and the transaction is completed using the magnetic stripe. There are a variety of legitimate reasons for fallback transactions, such as dirty chip reader or damaged card. Fallback transactions can also occur through a deliberate attempt by fraudsters to force magnetic stripe transactions. For example, a fraudster could damage the chip on a counterfeit card or cover the chip with tape so it cannot be read by the EMV-enabled POS or ATM terminal.

The liability for fraudulent fallback transactions is on the issuer for allowing the fallback transaction to occur. You can manage the risk by working with your card processor to develop rules for fallback transactions that fit your credit union's risk appetite at POS terminals and ATMs based on data points such as transaction amount, geolocation, merchant category code, etc.

Risk Mitigation

Credit unions should consider these risk mitigation tips:

- Educate your members to never give personal information over the phone.
- Credit unions that change debit card PINs through the call center should evaluate the security questions used to confirm the caller's identity. Avoid using easily defeated security questions. Instead, use an identity verification service in the call center. If this is not possible, credit unions should use strong out-of-wallet questions to verify the caller's identity.
- Credit unions offering VRUs allowing members to change debit card PINs are encouraged to require members to successfully pass all five security tests rather than just three out of the five.
- Monitor reports for fallback transactions, which are identified by a combination of POS entry mode, card service code and terminal entry capability.
- Work with your card processor to develop rules for fallback transactions and set daily spending and velocity limits.
- If you haven't already, implement EMV on all ATMs to reduce the liability of fraud for your credit union.

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. The Protection Resource Center requires a User ID and password. Review these resources to learn more:

- RISK Alert: PIN-Based Fraud on the Rise
- Protect Yourself – Member Protection Tips
- Fallback Transactions and EMV

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for white papers & checklists
- Webinars and Education
- RISK Alerts Library

Check out these areas of practice to help you manage pressing risks.

The Protection Resource Center requires a User ID and Password.

Interested in learning more about emerging risks or scams?
Contact CUNA Mutual Group's Risk & Compliance Solutions at **800.637.2676** or by email at riskconsultant@cunamutual.com for additional risk insights.