RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

ATM Shimming & Fallback Transactions Back On The Rise

ATMs are once again an easy target for fraudsters to capture card data – and, again, it is through shimming/skimming devices found on credit union-owned ATMs. Since the implementation of EMV/Chip cards, these devices have occasionally gone undetected leading to a large number of cards being compromised. The cards are used at other ATMs or through POS transactions where fraudsters rely on fallback transactions to override the EMV technology to obtain cash and/or merchandise.

Details

Fraudsters are once again attacking ATMs in hopes to capture card details and use them to create counterfeit cards. According to CUNA Mutual Group claims, fraudsters are often using shimming devices installed on ATMs to commit their fraudulent acts. Shimming devices became popular in 2018 when many cards transitioned to EMV.

A **shimming device** (photo attached from one recently found on a credit union owned ATM) can be very difficult to detect. The slim card-shaped device is wedged or shimmed into the card reader which allows it to read each card that is inserted into the machine.

Because the shimming device is out of sight and hidden within the reader; it can go virtually undetected by ATM users and even slip through the credit union's visual inspection of the ATM.

Once the card information is captured, the criminal creates the counterfeit card in which they use to target ATMs to obtain cash. They even may use these cards internationally. If the credit union allows **fallback transactions** at ATMs fraudsters are usually successful in using these cards. Considering that most merchants and card issuers have upgraded to EMV/Chip technology; thieves are relying on the use of fallback transactions to ensure these counterfeit cards can work at ATMs or POS terminals.

Keep in mind, a fallback transaction occurs when an EMV transaction is attempted at an EMV-enabled terminal, but the chip cannot be read. The transaction is then processed by falling back to the magnetic stripe on the card. Since these counterfeit cards do not have EMV technology, they will fall back to the magstripe on the card.

Fallback transactions are considered high risk, less secure transactions. They also eliminate any chargeback rights the credit union may have for a fraudulent transaction. Credit unions may consider if fallback rules are needed based on card usage.

Date: May 10, 2022

Risk Category: ATM; **P**lastic Card; Fraud; Scams; Consumer Payments

States: All

Share with:

- ☐ Branch Operations
- ☐ Executive Management
- ☐ IT
- ☐ Plastic Cards / Cards Department
- ☐ Risk Manager
- ☐ Transaction Services

Facing risk challenges?

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

ATM Shimming & Fallback Transactions Back On The Rise

Risk Mitigation

Credit unions should consider these mitigation tips:

- Block all fallback transactions, especially at ATMs. In addition, consider blocking all fallback transactions conducted internationally
- Set low daily dollar limits based on your credit union's risk appetite
- Eliminate ATM-only cards due to the lack of EMV technology available
- Ensure your ATM vendor utilizes anti-shimming technology and/or shimming detection technology that would automatically shut down the ATM if one is detected. Ensure this feature is enabled on all your ATMs as well.
- Conduct daily inspections of your ATMs, Use this ATM inspection checklist as a starting point
- Develop ongoing rules around fallback transactions by working with your processor
- Work with your processor to implement chip & pin for all POS transactions
- Educate staff and members of these shimming devices and encourage them to report anything unusual found at the ATM
- Educate members to cover their hand to hide their PIN when entering it at the ATM
- Ensure all credit union ATMs are EMV-enabled to accept chip cards
- Ensure your settings for EMV do not allow for fallback transactions at merchants when EMV terminal is detected

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.

- ATM Inspection Checklist
- ATM Safeguards

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.