intact financial services

# NEWS FROM THE VAULT

March 2019 | Issue 19

## ATM Fraud Alert

**BY CRAIG M. COLLINS – PRESIDENT, FINANCIAL SERVICES**

As the use and sophistication of technology increases, it would stand to reason that it would be more difficult for fraudsters to gain access to bank accounts via ATMs. Unfortunately, crooks seem to be equally sophisticated, and quickly outwit many safeguards soon after they are put in place. Here are some highlights and examples of ATM frauds that are unfolding across the country.

### Confirm that your ATMs are EMV Chip Enabled

A particular type of ATM fraud is showing up in many areas. It involves the use of foreign counterfeit cards being used at ATMs. While the cards used in the fraud have EMV chips, the ATMs that have been attacked were not EMV chip enabled. The fraudsters find the institutions without the EMV enabled ATMs, empty the cash with fraudulent transactions, and then drive to the next branch location (assuming that more of that particular bank's ATMs are not EMV enabled). The lack of EMV hardware shifts the financial liability for the fraud back to the bank that owns the ATM.

Confirm that your ATMs are EMV chip enabled. If not, you should consider restricting access of any cards that aren't issued by your bank, and call your ATM vendor to get the EMV hardware and software installed immediately.

### Cardless ATM Transactions

While they sound convenient, cardless ATM transactions are now the newest target of fraud.

*Fake Text Scam*: Customers can receive text messages "from the bank" that send them to a fake link. The customer is told that their account has been locked and they need to provide personal information. This information is then used to initiate and complete cardless ATM transactions.

*Cloned Phone Scam:* Many of these scams are originating while a customer is using unsecure public Wi-Fi. The fraudsters are able to gain login and account information as well as phone information. They use the information to clone the customer's phone or add a new number to the account to initiate transfers.

### ATM Security Suggestions

- Confirm that your ATMs are EMV chip enabled.
- Educate customers to use mobile banking apps on either their cellular network, or on a secure Wi-Fi network.
- Remind customers that the bank does not send "unsolicited" emails or texts.
- Limit cardless ATM withdrawals to a small dollar amount and limit daily usage.
- Limit the timeframe that a transaction code is viable.

- As it becomes available, utilize biometric identification (fingerprints, iris and facial recognition).
- Maintain usage of multi-factor authentication methods.