Fraud Alert Update February 3, 2016

ATM Fraud

LSC has received multiple reports of ATM fraud. The fraud has taken place at terminals within the Chicagoland area as well as Ohio, New York and Maryland. Other geographic areas may be targeted.

It is believed that skimmers have been placed on convenience store ATMs where your members are making legitimate withdrawals. The card and PIN are being skimmed and counterfeit cards are created and used at other ATM machines. Most of the fraudulent transactions are in the $200 to $400 range.

Best Practices for the Credit Union

- Ensure that your cardholders are aware of the existence of skimming fraud, how it is perpetrated, and how they can protect themselves.
- Encourage your cardholders to avoid suspicious or unfamiliar terminals wherever possible.
- Review daily limits for ATM transactions
- Place member communication on websites.
    - The chances of your cardholders getting hit by a skimmer are higher on the weekend than during the week, since it's harder for members to report the suspicious ATMs. Criminals typically install skimmers on Saturdays or Sundays, and then remove them before opening on Monday.
- File police reports based on where the fraud is occurring since cases are investigated jurisdictionally.
    - LSC has been working with the Secret Service as well as local law enforcement. If you are experiencing ATM terminal fraud, please contact LSC to report at lscriskmgmt@lsc.net.

Best Practices for Cardholders

The typical ATM skimmer is a device smaller than a deck of cards that fits over the existing card reader. Most of the time, the attackers will also place a hidden camera somewhere in the vicinity with a view of the number pad in order to record personal-identification-numbers. The camera may be in the card reader, mounted at the top of the ATM, or even just to the side inside a plastic case holding brochures. Some criminals may install a fake

PIN pad over the actual keyboard to capture the PIN directly, bypassing the need for a camera.

- **Check for Tampering**

  When you approach an ATM, check for some obvious signs of tampering at the top of the ATM, near the speakers, the side of the screen, the card reader itself, and the keyboard. If something looks different, such as a different color or material, graphics that aren't aligned correctly, or anything else that doesn't look right, don't use that ATM.

- **Wiggle Everything**

  Even if you can't see any visual differences, push and pull at everything

- **Protect the PIN**

  Even if you don't notice a skimmer and swipe your card, covering your hand when you enter your PIN can block a camera that may have been installed. If the keyboard doesn't feel right—too thick, perhaps—then there may be a PIN-snatching overlay, so don't use it.

  - **Location**

  Criminals frequently install skimmers on ATMs that aren't located in overly busy locations since they don't want to be observed installing malicious hardware or collecting the harvested data. Stop and consider the safety of the ATM before you use it.

As more information becomes available, LSC Card Services will continue to update the alert.