MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

August 16, 2019

ATM Skimming/Shimming

The use of ATM skimming and shimming devices to steal personal account information continues to be a growing problem for financial institutions. Criminals install skimming devices to ATMs to collect card data when the card is inserted. They are also collecting PIN information by using a small camera disguised as a legitimate component of the machine. To avoid detection, the devices are often installed and subsequently removed in a short period of time.

Criminals are increasingly targeting ATMs that are not yet Europay, MasterCard and VISA (EMV) enabled. EMV has been adopted by all major card networks since implementation. The EMV chip technology is a small square computer chip that creates a unique code for each transaction. The terminal reads the chip embedded within the card instead of the magnetic stripe on the back. The chip subsequently makes it much more difficult for criminals to capture the financial information due to the unique nature of coding.

In some instances, credit unions have upgraded to EMV technology but have not turned the EMV reader on. Additionally, fallback transactions – in which the financial institution allows the transaction to fall back to the magnetic stripe on EMV cards has been an issue. ATM processors must validate and code the transaction as EMV. Criminals are picking up on card issuers that have not turned the fall back option off and use this to their advantage as the card data is easily stolen from the magnetic stripe.

With a recent trend across the country of ATM skimming, the MCUL has prepared the following risk mitigation guidance to assist credit unions in combating ATM fraud.

Risk Mitigation

The following are some risk mitigation tips for credit unions to consider:

- Ensure all ATMs are EMV-enabled and can accept chip cards by consulting with your ATM vendor
- Check with your processor to ensure that each of your credit union's ATMs have EMV capability turned on and verify transactions are properly coded for EMV
- Discuss with your ATM servicer and consider implementing any new ATM fraud prevention technology
- Adopt or review fallback strategies and ensure proper coding for EMV
- Conduct regular (recommended daily) inspections of your credit union's ATMs. Look specifically for:

- *Skimming overlay devices:* These devices are placed over the card slot.
- *Shimming technology:* This is a thin, card-sized device with a microchip into the card slot that isn't visible from the outside of the machine.
- *Keypad overlays:* These devices are placed over an ATM's keypad and captures PINs as they are entered.
- *Tiny "pinhole" cameras:* These cameras are used in conjunction with the skimming or shimming device. The camera is placed in a location on the ATM to record the user entering the PIN. Criminals may even use these cameras with thermal imaging to see the numbers and order in which they were pressed.

Incident Response Tips

- *Create a plan*: As with any potential risk or threat to the credit union there should be a plan for what to do should a skimming device be found on one or more of the credit union's ATMs.
- *Document the plan***:** Include each action that should occur and people to be involved.
- *Employee training:* Ensure all employees are trained on what to do and not do if a skimming device is found.
- *Work with third party vendors and servicers:*
  - Ensure third party vendors and servicers are also monitoring ATMs.
- *Inspect ALL locations:* Frequently check all ATMs surfaces and surroundings for anything suspicious.
  - If able, have someone check ATMs on off hours and weekends as these are oftentimes when skimmers are installed.
  - Review ATM footage for off hours and weekends.
  - Ensure ATMs are well lit and maintained (particularly ATM cameras).
  - Remain diligent with inspections – establish and maintain a schedule.

- *Establish ATM standards:* Create visual standards for all ATMs and include in the standards;
  - *Photograph each ATM* – show employees what it should look like so ATMs may be quickly examined for anything that may seem out of place.
- *If a skimmer is found:*
  - Contact law enforcement.
  - Do not remove the device.
  - Secure the area and close the ATM(s).

In 2013 former Michigan Governor Rick Snyder signed House Bills 5050-5054 which harmonized existing criminal sanctions for card skimming into one felony provision. The bills also amended jurisdictional statutes to ease prosecution for skimming offenses and criminalized the sale or possession of skimming devices.

Should you have any questions or need additional information, please contact Sarah Stevenson at 800-262-6285, ext. 494 or Sarah.Stevenson@mcul.org