Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

Are Your ATMs Safe?

SUMMARY

The number of attacks on financial institution's Automated Teller Machines (ATMs) is rising. Below we address each type of attack and outline best practices to protect against bad actors targeting your machines.

HOW THE ATTACKS ARE PLOTTED & RISK MITIGATION STEPS

I. **Skimming/Shimming** - Bad actors deploy skimmers, sometimes referred to as shimmers, on commonly used devices such as gas pumps, point of sale (POS) devices, and ATMs. Along with the skimmers, bad actors will often install small cameras or keypad overlays that will allow them to capture the PIN for use in further fraud. With the skimmed card data, the bad actors can create counterfeit cards.

There are three main types of skimming devices that impact ATMs:

1. Overlay skimmers that attach on the outside of the ATM
2. Throat skimmers that attach on the inside of the ATM
3. Deep insert skimmers that go into the ATM card reader

Risk mitigation steps:

- Work with your ATM manufacturer to ensure that the most up to date anti-skimming hardware and/or software is in place. There may be additional hardware and/or software that is available to defend against the three main types of skimming devices.
- Ensure the ATM will shut down if a skimming device is detected.
- Blocking fallback transactions at ATM and POS will prevent counterfeited cards from functioning.
- Educate members on skimming devices and provide a reporting process.
- Inspect ATMs daily, including camera footage.
- Notify law enforcement immediately if you suspect there is a skimming device installed on your ATM.

II. **Hook & Chain Attacks** - These types of attacks continue to occur nationwide. To conduct the scheme, the bad actors utilize brute force to steal funds from an ATM. The bad actors typically use stolen trucks with tow hooks inserted into the ATM attempting to open the vault door or remove the ATM from the ground entirely. The scheme is costly to a victimized financial institution. Even if the bad actors are unsuccessful in accessing the cash the physical damage often deems the ATM a total loss.

Risk mitigation steps:

- Work with ATM manufacturer to ensure safe door is protected against hook and chain attacks.
- Install a safe slot reinforcement kit.
- Encase the ATM or install security gates or bollards at ATMs to make it difficult for the bad actors to access the ATM.
- Ensure ATM is hooked up to an alarm system. Alarming the top hatch and fascia doors will start the dispatch process sooner.
- Install strobe lights and sirens to ATMs as well as additional exterior cameras as further deterrent.
- Consider relocating ATM from the furthest drive-thru lane.

III. **Jackpotting** - Jackpotting was first prevalent in the United States in 2018. Activity seemed to dissipate for a bit, however we have recently seen an uptick in financial institutions facing jackpotting events. Jackpotting involves a bad actor installing malicious software and/or hardware onto an ATM that enables the bad actors to take control of the ATM and cause the machine to dispense large volumes of cash.

Risk mitigation steps:

- Monitor ATMs closely to detect any suspicions of tampering.
- Use a high-security lockset for the hood of the ATM versus the standard lock.
- Ensure the hood is tied into the alarm for the ATM.
- Install an audible siren and strobe light that will go off if the ATM is opened while armed.
- Use strong passwords, make sure it is not the default password
- Create a whitelist to prevent unauthorized applications from being installed.
- Encrypt the hard drive.
- Make sure the ATM is included in software updates and security patches.

RISK MITIGATION RESOURCES

- Follow this checklist to assist you as you inspect and assess the physical and alarm security of existing or new purchases of ATMs/ITMs. Download *Security Checklist for Standalone ATMs & ITMs here*.
- For additional insight, review our recent risk alert, *Fallback Authorization on Card Present Chip Cards*.