EVOLVING BREACHES IN DATA SECURITY

We live in a modern era. A world of information is at our fingertips, and those in the financial industry have to remember that hackers and thieves have access to much more information about systems, software, and internal processes than they've ever had before.

Today's criminals can find, purchase, or download any details they need to plan an attack of any kind, whether their modus operandi is physical or data-related. That means financial institutions have to be prepared to fight on every front — which can quickly become incredibly complex. ATM attacks fall into two categories: physical or logical.

PHYSICAL ATTACKS

Physical ATM attacks are focused on extracting cash from ATMs. These types of attacks happen quickly and often cause a lot of damage to ATMs and locations in the process. Some of the most common physical attacks are:

- Ram-raids, Pull Outs, Smash and Grabs - Each of these attacks are similar and typically involve using a truck or vehicle as a ramming device to gain entry to a location, physically removing the ATM, then later breaking into the safe and emptying the cash cartridges.
- Cutting, Drilling, Wedges, Crowbars, and Hydraulic Tools - These types of attacks typically occur at soft targets, where the ATM can be accessed quickly, and high-grade safes do not protect the cash cartridges. These attacks involve quickly gaining access to the cash without removing the ATM from its location.
- Explosive Attacks - Less common, these extremely dangerous attacks involve using gas or solid explosives to blow up the ATM to access the cash.

LOGICAL ATTACKS

Logical ATM attacks typically have two objectives: 1. Collect cardholder information; 2. Manipulate data to withdraw money from the ATM fraudulently. Criminals are always looking for new ways to access cardholder data and to steal money from vulnerable ATMs. Below are some of the logical attacks being used by criminals.

- Jackpotting - This refers to emptying all of the money from an ATM. Jackpotting can occur in two ways: 1. By gaining control of the bill dispenser and sending it a command to dispense cash. 2. By using a device to intercept and manipulate data being exchanged between the ATM and the payment processor to commit fraudulent transactions.
- Black Box, or Man-in-the-Middle - As described above under "Jackpotting," these attacks involve using a third-party device to intercept and manipulate data being sent between the ATM and payment processors to empty some or all of the cash from the ATM. These devices can also be used to read and log cardholder information.
- Network Packet Sniffing, or Eavesdropping - These types of attacks use a computer program or computer hardware to intercept and log data being communicated over the ATM network. The data collected can then be used to coordinate and plan other

types of attacks on the ATM or to defraud those who have used the ATM to withdraw cash.

- Malware - Once installed on an ATMs hard drive, malware can intercept and manipulate data to commit man-in-the-middle or jackpotting attacks and can also log sensitive cardholder information. To install malware, criminals typically need to gain physical access to the ATMs computer hard drive.
- Skimming, Deep-Insertion Skimming, and Shimming - Designed to read and steal cardholder information and personal identification numbers (PINs), these attacks involve attaching or inserting devices to or inside ATMs to read and store data from the cards. Fake debit cards, or clones, are created using this information. False PIN pads and cameras are also often used to record the user's PIN.

SECURITY TIPS

While there are several types of ATM attacks, there are just as many security products available on the market to protect against them. The first lines of defense against ATM attacks, however, only costs your time.

Completing a thorough site assessment of prospective ATM locations can be one of the most effective ways to avoid falling victim to ATM attacks. Consider contacting local law enforcement agencies to inquire about crime rates in the area. Interview surrounding business owners and employees to determine whether or not theft and vandalism is a common occurrence in the area.

Additionally, consider the physical characteristics of the location itself. If answers to the following questions are not favorable, you may want to reconsider placing an ATM at the site:

ASSET PROTECTION – SITE ASSESSMENTS

	Can the ATM be positioned in a high visibility area and within the line of site of employees?
	Does the site maintain a functioning security camera system?
	Is the site equipped with its own alarm system and alarm monitoring service?
	Can the ATM be positioned away from easy access points such as doors, windows and exterior walls?
	Is the building constructed from solid materials? (metal, concrete)
	Can the ATM be bolted to the floor or frame of the building?
	Can staff access to perform regular site visits to ensure it hasn't been tampered with?

Other elements to consider in protecting your valuable assets and customer data include:

1. The use of software/behavioral analytics that recognize anomalous or out-of-character behavior for the cardholder. An example of this might be the usage of a card at an ATM the holder never, or rarely, visits or withdrawal amounts and transaction times that are not consistent with the cardholder's patterns.
2. Regularly download patches and software updates for Windows-based ATMs. In a perfect world, these systems should push down security patches weekly.
3. Ensure that networks are secure, so if one ATM is hacked, fraudsters can't infect the entire ATM system - or worse, the whole corporate network.
4. Monitor the system for unapproved software changes. Have controls in place that detect when the system itself has been manipulated or changed.

The utilization of security mechanisms which detect changes to the physical or electronic characteristics of your asset can also be an effective deterrent. These include:

1. Jammers: Devices that protect via an electromagnetic field that "jams" or disables skimmer devices.
2. Sensors - Physical sensors send an alert when a door opens, tilting and vibration are registered, the power source is cut, or other signs of physical intrusion or tampering is detected.
3. Penetration mats - Similar to sensors, penetration mats installed on the fascia of an ATM can alert you if someone is attempting to cut or drill into it.
4. Anchoring devices - Bolting an ATM to the floor or securing it to the frame of the building using an anchoring device is an effective way to deter thieves from attempting to steal an ATM.
5. Security collars and anti-lasso devices - Security collars and anti-lasso devices are designed to stop thieves from being able to place a rope or chain around the ATM.
6. Tracking systems - In the event of an ATM theft, the ATM's location is tracked and shared with local law enforcement.
7. Intelligent banknote neutralization systems (IBNS) A.K.A. Dye or Ink Packs - Intelligent banknote neutralization systems render banknotes unusable by thieves.
8. Audible alarms and sirens - Predefined criteria or a remote command can trigger alarms and sirens.

Finally, the key to genuinely reducing your risk should ultimately include multiple layers of security. Ensuring these layers work in sync, along with associate-based interactions such as service technicians inspecting for skimming devices and employees conducting random physical checks of the ATM and the surrounding area, are the best methods to maximize your security and limit potential breaches of company or customer data.

ABOUT TELLEREX

Tellerex is committed to leveraging our knowledge and experience to reduce atm expenses, increase reliability, and accelerate a contribution to your company's bottom line. Contact us to learn how our complete ATM management solution can simplify the end-to-end process and required oversight for your ATM and cash recycler networks.