PROTECTING ATM CLIENTS AND ASSETS

GMR 410, LLC

PREPARED BY:

Mary Gates, CFSSP, CHPA-III
Vice President of Security

Trusted Advisors | Trusted Solutions

INTRODUCTION

How well do you understand the issues related to ATM crime? The more you know on this topic, the better equipped you will be to take action to deter criminal activity, thus protecting your clients and your assets.

In this white paper, you will learn about the different types of ATM related crime, applicable state regulations, and how to manage the security of your ATMs to reduce incidents.

CONTENTS

BANK SECURITY OVERVIEW

Financial institutions are responsible for ensuring that a written Security Program is developed and implemented, and for designating a Security Officer to carry out certain security responsibilities. The Security Officer is ultimately accountable for setting the strategic direction and governance across the financial institution for Physical Security management. This responsibility should be fulfilled through a risk-based framework that provides physical security solutions aptly designed in accordance with industry practices and administered to mitigate against the risk and threat environment.

Further, the Security Officer is responsible for designating Security staff and additional resources to implement and manage a risk-based Program of Policies, related Standards, and associated security operational Procedures. This Program, referred to as the Security Program, should be designed to safeguard the human and physical assets of the financial institution and any subsidiaries, affiliates and related entities. Utilizing an ongoing assessment program to monitor and respond to changing risks and threats is a prudent step for Security Officers to address the critical challenge of ensuring the protection of their people, assets and information.

ATM CRIME

Since the invention of the ATM, criminals have evolved their methods to successfully obtain cash and steal customer data. ATM owners and operators are vulnerable to a variety of threats including physical and malware or software-targeted attacks. There are many types of ATM crime, including:

- Physical attacks, including smash and grab or ram-raid attacks, and explosive gas attacks
- Logical attacks, such as ATM Jackpotting and Black Box Attacks
- Fraudulent attacks, including Skimming and Cash Trapping
- Customer attacks, involving kidnapping, forced withdrawals, robberies and assaults

PHYSICAL ATTACKS

Physical attacks consist of any traditional robbery technique used to remove cash or other valuable media from the ATM by physically breaching the enclosure or vault and obtaining the cash or the currency cassettes.

A common form of attack – the “smash and grab” – is to remove the ATM to another location. In these physical attacks, the tactics are typically destructive to more than the ATM, often damaging buildings or other structures in proximity to the ATM.

Recent data from the European Association for Secure Transactions (EAST) reports physical ATM attacks continue to increase and have typically focused on using gas to blow up the ATM. Evidence also indicates an increase in the use of solid explosives such as C4, explosive gel and dynamite. The United States has begun to experience ATM attacks using explosive gas, including attacks in San Diego, Burbank and Los Angeles.

CUSTOMER ATTACKS

Customer robberies/assaults typically do not result in a large pay-day for a criminal; however, the consequences are far reaching. In addition to the physical and emotional harm suffered by the customer, the bank could face brand and reputational damage, premise liability and significant financial damages.

LOGICAL ATTACKS

Logical attacks on ATMs are comprised of malware, software and cyber-related thefts. These types of attacks use technology to exploit features on an ATM which would not have been considered vulnerable at the time of manufacture.

ATM JACKPOTTING

ATM jackpotting involves the suspect inserting removable media into the ATM's main board and initiating a reboot function by breaching the top of the cabinet which houses the computer used to control the terminal. The ATM will boot to the inserted USB, DVD or CD, allowing malware to be copied to the ATM main board. Malware attacks can be initiated when the ATM is online, using a USB device with auto play enabled or a stolen Windows Administrator password.

Once the malicious program is loaded, the criminal can gain remote access and initiate a dispense function. Due to the nature of these attacks, several ATMs can be targeted simultaneously, leading to substantial losses for the financial institution or ATM deployer.

BLACK BOX ATTACKS

Black Box attacks also require breaching of the cabinet. In this type of attack, the suspect will access the cash dispense cable, bypass the main board communications and connect a periphery device directly to the dispenser. The suspect is then able to initiate the dispense command.

SKIMMING

Skimming is a fraud which involves the use of electronic devices to steal personal information stored on debit cards. Through physical attachments, suspects record the magnetic strip on a debit card. The devices utilized are smaller than a deck of cards and are fastened in proximity to, or over the top of the ATM’s card reader or the entry door reader.

PIN-Capturing refers to a method utilized by the suspects of strategically attaching cameras and various other imaging devices to ATMs in order to capture the user’s PIN. Once captured, the electronic data is encoded onto fraudulent cards and the cards and captured PINs are used to withdraw money from customer accounts.

CASH TRAPPING

Cash trapping methods vary, from simple devices attached externally to complex, electro-mechanical devices inserted into the dispenser of the ATM. The criminal utilizes the device to prevent cash from being dispensed to legitimate users.

Because there are numerous methods to trap cash, to include placing the ATM out of service, there is no simple solution to address every method employed by criminals.

STATE REGULATIONS

Currently, 13 states and 2 cities [i] have specific laws establishing standards to address ATM safety. These measures outline requirements including but not limited to customer disclosures, lighting and landscaping and, in some cases, the use of cameras, mirrors or other security. Additionally, numerous states and other cities require safety measures to be considered, but do not necessarily specify the minimum measures [ii]. New and updated legislation or regulations are proposed from time to time.

State Regulations in CA, GA, IL, NV, OR, TX and WA further include a requirement for ATM operators to adopt a procedure for evaluating safety of the ATM. This includes the incidence of crimes of violence in the immediate neighborhood of the ATM, as reflected in the records of the local law enforcement agency and of which the operator has actual knowledge.

Unfortunately, none of the State Regulations define “immediate neighborhood.” Furthering the problem, there is currently no uniformity in how law enforcement reports crime data[iii]. Some municipalities report by “beats”, others by “area” or “block.” Still others report at the county level. This inconsistency results in questionable statistics which may fail to promote measured security planning and informed decisions for needed security measures.

PROTECTING YOUR ATMs

ATMs are lucrative targets for criminals. Accordingly, it is incumbent upon ATM operators to take an active role in protecting customers, deterring losses, and ensuring brand reputation. Using a layered approach to protect ATMs, operating systems and customer data ensures that if one security feature fails, another will be in place to protect the ATM and the associated assets.

PHYSICAL ATTACK DETERRENCE

- Conduct risk assessments to identify the potential for crime at your ATMs and branches.
- Implement an ATM lighting and landscape program and conduct regular assessments to ensure compliance with state regulations and internal standards.
- Increase physical security by installing ATMs in areas of high-visibility and utilize, where appropriate, additional features such as bollards, steel plates, floor-bolting, additional cameras or high-curb structures.
- Where appropriate, introduce security technology enhancements such as alarms or other systems that detect cutting, grinding, drilling, hammering, pull-out or explosive gas attacks. In addition to alerting the monitoring center, some of these technologies will activate sirens, flashing lights and display messages on the ATM screen to alert that the attack has been detected.
- Use GPS technology to track an ATM or currency cassettes if removed due a successful attack.

LOGICAL ATTACK PROTECTION

- Introduce additional physical security to reduce access points and access to the computers through the surround or top hatch.
- Update passwords for backend ATM access.
- Lockdown the operating system.
- Whitelist appropriate programs.
- Disable boot and auto-run features.
- Ensure the ATM fleet remains up to date with current versions of all software and related patches.
- Stay up to date on the latest technologies and services that keep ATMs protected as threats evolve.
- Ensure you are running the latest software and patches are installed as soon as they are deployed.

REDUCE JACKPOTTING

- Take advantage of innovations in multifactor authentication.
- Use unique serial numbers to identify each cabinet lock and associated key.
- Maintain a database to track which ATM and location requires a specific key and the person(s) with access to the specific key.
- Clearly document processes and procedures related to issuing and replacing lost or stolen keys.
- Use strong passwords, ensure firewalls, anti-malware protection and terminal whitelisting solutions are correctly configured.
- Disable the ability to boot or auto run from any USB device or CD/DVD drive.

DETERRING BLACK BOX ATTACKS

- Use available communications encryption for cash dispensers to ensure that black boxes cannot control dispensers.
- Use a physical barrier over holes and vents that are near or in direct line of sight to sensitive components such as USB ports, communication sockets, card reader electronics and dispense cables.
- Monitor the ATM fleet, and take note of unusual patterns in power outages, resets and communication failures is a critical line of defense.

GUARD AGAINST SKIMMING

- Implement EMV[iv] capable readers; however, until magnetic stripe cards are completely phased out, skimming will continue to occur.
- Engage in regular monitoring to ensure a device has not been installed.
- Where to spot skimming devices:
  - Door Reader
  - Light Diffuser Area
  - Speaker Area
  - ATM Side Fascia
  - Card Entry Slot
  - ATM Keyboard Area

PREVENT CASH TRAPPING

According to ATMIA's Best Practices for Preventing Cash Trapping, solutions vary widely based on the physical characteristics of the ATM. While there are some third-party solution providers who have specialized security solutions for specific models, general enhancements and upgrades include:

- Adding enhanced fascia plates and components to deter attachments
- Monitoring to detect abnormal activity during and post-transactions
- Live-monitoring of activity in areas of highest risk
- Regular inspection of the ATM fleet (for sticky residue)

ABOUT US

As a solutions-based security consulting firm, GMR 410 LLC[v] can help identify your vulnerabilities, tailor solutions and help you keep your assets, employees, customers and third-party service providers safe.

Visit www.gmr410.com to learn more about our security services or visit www.gmr1.com to learn about our ATM lighting and compliance solutions. GMR 410 and GMR Protection Resources, Inc. are diverse supplier, WBENC certified woman owned and operated businesses.

ENDNOTES

[i] CA, DC, FL, GA, IL, LA, MD, NV, NJ, NY, OR, TX and WA. The LA, OR, and WA statutes also include the Night Depository. Cities with ATM specific laws include New York City and Strongsville, OH.

[ii] AL, CT, MA, MN, MO, NM, RI, VA and WY. Cities with non-specific laws that do not establish safety standards include Orange, CT and Sharon Hill, PA.

[iii] Effective January 1, 2021, the Federal Bureau of Investigation will retire the Summary Reporting System (SRS) component of the Universal Crime Reporting Program and will require all law enforcement agencies to move to the National Incident-Based Reporting System (NIBRS).

[iv] EMV stands for Europay, Mastercard and Visa. The United States began migrating to EMV chip cards in late 2015, but the technology was widely used in Canada and Europe prior to its adoption in the United States.

[v] GMR410, LLC is a wholly-owned subsidiary of GMR Protection Resources, Inc. Both companies are headquartered in Heath, TX. Info410@gmr1.com