FINANCIAL SERVICES | Information Sharing and Analysis Center

Understanding ATM Attacks

28 August 2018

This product was created as part of a joint effort between the Financial Services – Information Sharing and Analysis Center (FS-ISAC), the American Bankers Association (ABA), the Credit Union National Association (CUNA) and the Independent Community Bankers of America (ICBA).

American Bankers Association®

CUNA® Credit Union National Association

ICBA Independent Community Bankers of America®

Understanding ATM Attacks

In response to media reports concerning cyberattacks leveraging Automated Teller Machines (ATMs), Financial Services Information Sharing and Analysis Center (FS-ISAC), American Bankers Association (ABA), Credit Union National Association (CUNA) and Independent Community Bankers of America (ICBA) developed this paper to explain how cybercriminals conduct attacks and actions financial institutions may take to protect consumers.

Attacks Against ATMs

Cybercriminals target ATMs through both physical and computer-based means to steal funds for a cybercrime gang or a nation-state. These attacks often occur around holidays in an attempt to circumvent or delay detection. This may involve the creation of fraudulent payment cards at one or more financial institutions.

Four Types of ATM Attacks

- Skimming attacks – Skimmers are devices that may sit on top of the ATM PIN pad and/or card slot or they may be inserted deeply into the card slot. Sometimes, criminals use a camera to capture a consumer’s PIN as it is entered. Usually, the information captured from the skimmer and camera is used to create cloned cards.
- Shimming attacks – These are similar to skimming attacks, except that criminals use special mechanisms inserted deeply within the ATM to capture the chip information on newer chip-enabled cards. Again, this information is used to create cloned cards.
- Cash-out schemes – Criminals use ATMs either locally or globally to drain funds from multiple accounts held at one financial institution. These attacks use legitimate card numbers that were stolen in another campaign and involves the manipulation of the account balances and withdrawal limits to perform the theft. This attack is also referred to as an “unlimited operation”.
- Jackpotting attacks – Like it sounds, in this attack criminals use physical and/or logical methods to force one ATM to dispense all the cash, just like a slot machine.

Common Misunderstandings About ATM Attacks

In many cases, the news media assumes that attacks against ATMs, no matter the type, result in the loss of funds to customers. However, most ATM attacks do not result in the loss of funds to customers as a result of consumer protection laws and business practices. The primary target of cash-out schemes and jackpotting, for example, is the financial institution, not consumers’ accounts. That said, if criminals have used legitimate payment card information (e.g., numbers, PINs), then the financial institution will replace the funds and may reissue cards for its customers. This is protection for both the institution and the consumers whose accounts were affected.

How Institutions Protect Their Consumers’ Accounts

Financial institutions around the globe are experienced at information security and leveraging industry best practices. Your financial institutions’ customer protections likely include the following:

- Encryption of confidential information;
- Restrictions on who can access systems where confidential information is stored;
- Requirements for more than one person to approve high-risk procedures;
- Systems that will detect and prevent network intrusions;
- Settings and rules to prevent the loss of sensitive data;
- Anti-virus and anti-malware applications to prevent malicious files from infecting the systems;

- Programs that will prevent unauthorized applications or files from running on workstations;
- Monitoring for anomalous behavior or activities on networks and ATM systems;
- A regular cycle to manage patching or updating systems;
- Alerts that will notify institution staff if of abnormal activity, such as an ATM being disarmed or disabled; and
- Implementation of chip and PIN procedures for debit cards.

It is part of an institution’s cybersecurity program to keep the specific protections and programs they use confidential. However, FS-ISAC works with a large number of financial institutions domestically and around the world, helping them determine the best security practices to put in place and connecting them with their peers for further recommendations and insights.

Steps Consumers Can Take

Customers are not responsible for unauthorized charges; however, there are steps consumers can take to help protect their accounts.

- Protect your debit and/or credit cards at all times; don’t share cards or PINs with others.
- When using ATMs, be aware of your surroundings. Before using the ATM, look closely at the card slot and PIN pad for any abnormalities and glance up and around to see if you notice any cameras. If anything looks strange or unusual, do not use the ATM.
- If you notice odd or peculiar behavior by others at an ATM (inserting a cable or using multiple cards to withdraw funds at one time), contact local law enforcement and the institution; do not use that ATM.
- Be aware that institutions usually won’t contact you via text message or email about your debit or credit card, unless you have previously agreed to this method of communication; if you receive a suspicious text or email message claiming to come from your financial institution, contact your institution to check the legitimacy using the number on the back of the card.
- Be aware that phone calls you receive may not actually be from your bank or credit union. You should not provide the full card number, PIN or CVV code over the phone. When in doubt, call the number on the back of your card to verify contact.
- Be on guard against phishing attacks and do not open attachments or click links in emails you were not expecting.
- Use two-factor authentication and other security features offered by your financial institution to protect your accounts.
- Sign up for text or email alerts from your financial institution for certain types of transactions, such as online purchases or transactions of more than $500.
- Notify your FI as soon as possible if you suspect that your card PIN or electronic banking credentials have been compromised.
- Review account statements for any transactions you do not recognize; promptly notify your FI if you notice any unauthorized account activity. A small transaction (e.g. $0,01 or other small amounts) may be indicative of a criminal “checking” the card information to see if it is legitimate. A larger fraudulent charge typically follows.