Attacks against ATMs

Cybercriminals target ATMs through both physical and computer-based means to steal funds for a cybercrime gain 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 devises 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 form 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.

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 test 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 on 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 you 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 statement for any transaction 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.