ABA Insurance Services | MEMBER OF GREAT AMERICAN INSURANCE GROUP

SafeAlert®

ATM "Jackpotting" attacks have increased.
Criminals are using master keys and endoscopes to get into ATMs.

ATM attacks have been rampant since 2018 and are showing no signs of letting up.

For several years, "hook and chain" attacks were the most common method of ATM theft. To mitigate risk of this type of theft, many banks erected physical barriers.

More recent incidents, however, involve individuals using generic or master keys to unlock a machine's exterior chassis or endoscopes to get inside an ATM. No trucks required.

Shockingly, these can easily be purchased on the internet. The criminals then tamper with the machine's hard drives to install malware, ultimately resulting in the disbursement of cash. This is known as ***"jackpotting"—altering the ATM mechanisms and typically inserting malware to cause the machine to dispense cash to unauthorized users.***

The U.S. Secret Service has reported an increase in ATM jackpotting over the last six months. The attacks are believed to be the work of organized criminal groups and target multiple ATM manufacturers.

With generic or master keys, criminals access an ATM's chassis and remove and/or install malware using various methods such as a USB port device which then allows them to reboot the onboard PC using the compromised media and issue dispense commands, allowing them to deplete the ATM of cash. These commands can be sent remotely using either a laptop or cell phone, allowing them to avoid engaging directly with the ATM machine. In some cases, magnets are also used in conjunction to unlock an ATM's exterior.

In one such case, security video captured images of several people repeatedly accessing an ATM and removing large amounts of cash. The individuals were staged in a nearby parking lot and made a total of 48 trips to the ATM. It is suspected that the thieves had a master key, a small gold key with a rounded base and teeth on both sides, that allowed them easy access to the machine. Police ultimately apprehended the individuals and found a mobile wi-fi device, laptop, and USB cables in their vehicle.

Thieves may also use an endoscope *(similar to the slim, flexible instrument used in medical procedures)* to reach the internal mechanism of the machine, where they can attach a cord that allows them to sync their laptop with the ATM's computer. After installing malware, the perpetrators will contact co-conspirators, who can remotely control the ATMs and force the machines to dispense cash. Such mechanisms can dispense a hundred bills in about a minute.

Endoscopes are very easy to obtain. The image to the left is one of many examples that we found available to buy online through a very popular shopping site.

To mitigate risk of loss, financial institutions should proactively work with their ATM manufacturers to ensure that all machines in use are up to date on current security protocols. This should include:

- Limiting physical access to ATMs
- Installing machine specific keys to avoid easy access through master keys
- Implement additional access controls for service technicians
- Ensure ATM hard drives are encrypted
- Ensure network communications use TLS encryption
- Ensure that all components (operation system, firmware, software, etc.) include the latest updates
- Consider installing an ATM alarm to help detect an attack and ward of criminals
- Ensure alerts are triggered when an ATM goes off-line with a more immediate response time
- Neutralize cash to make it unusable to attackers through the use of cassettes with ink-staining solutions

Visit abais.com for more loss control information or to view this SafeAlert® online. To subscribe to SafeAlert, request reprints or if you have questions about this bulletin or other general loss control articles, contact marketing@abais.com or 800-274-5222.