

White Paper
2025

Armor Your ATMs:

A Proactive Defense Against
Evolving Threats

A strategic guide to detecting, deterring, and defeating sophisticated physical and logical ATM attacks.



Table of **Contents**

3	ATM Security Considerations
4	Secure the Cash with Upgraded Safe Strategies
5	UL and CEN Safe Cross Section Comparison
6	Secure Machines with Additional Protection
8	12 Tactical Tips to Prevent Jackpotting
13	Alarm and Camera Security Features
15	How Artificial Intelligence is Enhancing ATM Security
16	Summary
17	About Allied Solutions

ATM Security Considerations

When planning and installing new ATMs, it's important to consider the location, general security and risk surrounding the site. All ATM sites should be assessed for risk, regardless of their location – whether in-branch or off-premises.

ATMs located in-branch may be less vulnerable to certain attack vectors as they benefit from the security of the branch and the ATM is unavailable once the branch is closed, whereas standalone drive-up ATMs have a higher risk of attack. One common type of physical attack is the **“hook and chain”** method — where criminals use a hook and chain attached to a vehicle, like a pickup truck, to pull the ATM off its foundation — often targeting standalone, drive-up ATMs. Typically, the ATMs most vulnerable to this type of attack are positioned at the furthest drive-up lane, especially if there is ample space behind them for a getaway.





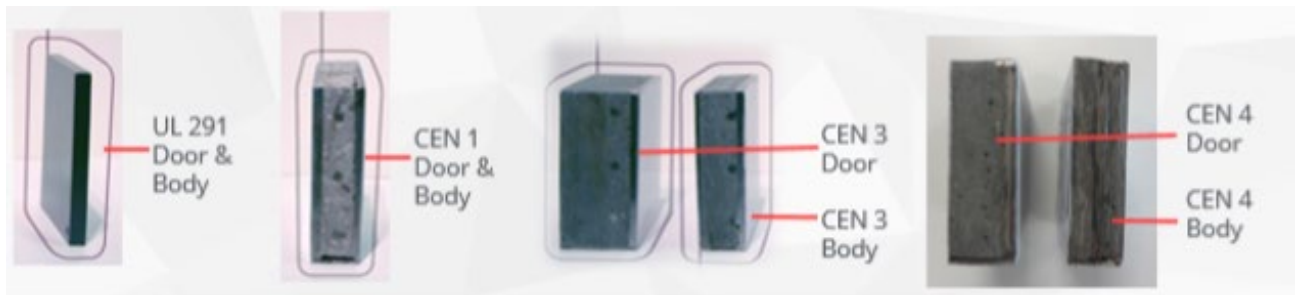
Secure the Cash with Upgraded Safe Strategies

ATM safe strategy has evolved, with the recommendation shifting from Underwriters Laboratories (UL) rated safes to Central European Norm (CEN) safes.

Unlike the UL safes made of steel construction, the CEN safes are constructed with a composite of steel and concrete, offering greater resistance to tool attacks. Plus, CEN standards provide a framework for testing and classifying the burglary resistance of ATM safes.

The higher the CEN grade the more reinforcement within the safe body and door, in turn, the greater resistance to tool attacks such as grinders and acetylene torches. Gas explosive protection is available for CEN 3 and CEN 4 safes. As threats targeting ATMs grow, CEN 3 with gas explosive protection should be the minimum protection for standalone drive-up island units.

UL and CEN Safe Cross Section Comparison



CEN 3 and CEN 4 GasEx safes offer enhanced security features, including:

- Same physical space model, maintaining the existing service footprint
- Improved bolt work featuring fixed bolts on the hinge side to resist explosions (preventing door ejection after hinge breach)
- Enhanced barrier materials for greater structural integrity
- Improved weld surfaces on the lock chambers and safe walls/doors
- A sensor, typically an explosive gas detector, connected to a canister containing an explosion-suppression chemical that, when activated, neutralizes the gas by altering its chemical composition
- A sensor, typically an explosive gas detector, connected to a system designed to dissipate the explosive gas and replace it with an inert gas
- A sensor, typically an explosive gas detector, connected to a system that floods the ATM safe's interior with fast-setting foam
- A device that, when triggered before gas concentration reaches critical levels inside the ATM, prematurely ignites the gas in a controlled manner
- Explosion-absorbent materials installed inside the ATM safe to dampen the shock waves generated by a detonation.

Organized gangs increasingly carry out **gas attacks** on ATMs because they are both lucrative and relatively easy to execute. This method has become well-established in certain criminal circles, leading to a rise in incidents. The financial impact extends far beyond the cash stolen—the cost of repairing or rebuilding damaged premises often exceeds the ATM's contents, with total losses per attack potentially [reaching six figures or more](#).



Secure Machines with Additional Protection

Consider these protection measures to enhance security on ATM and ITMs.

A **security kiosk** is specifically designed to deter "smash and grab" criminals. It should be constructed from steel and include an anti-ram base plate.




Loktec patented body armor packs (patent number GB2478534) provide the ultimate safe upgrade, providing physical and visual protection. [Loktec armor packs are available](#) for the ATM safe door, safe sides, and safe front to provide individual protection for all areas that are commonly attacked. These offer protection against cutting or tool attacks only—not explosive attacks.

Secure the ATM with a solid **steel security gate** designed to withstand violent physical breaches.



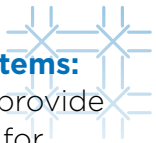
Other Essential ATM Protection Measures:

Alarm Monitoring:




Integrated alarms monitored 24/7, combined with an electronic lock, provide essential added protection to the ATM security gate or kiosk. Choosing an advanced system that offers immediate alarm activation and instant notification to your security provider and law enforcement helps elicit a speedy response to potential threats. Many monitoring systems are equipped with open, close, and heat detection capabilities, triggering the alarm before an attack can be completed.

ATM Anchoring Systems:



Anchoring systems provide essential protection for units at higher risk of ram raid or pull-out attacks. Anti-ram raid plinths have various designs, including a concertina-effect to absorb shock loads allowing the unit to be pulled but not fully removed from its mounting. These have been rigorously tested against heavy plant machinery, large 4x4 vehicles, and car transporters.

Enhanced Dispenser Shutter Assembly:



This mechanism is designed to harden shutter assemblies against cash trapping attacks. The reinforced materials combined with blocking sensors on the shutter offer greater protection against forced entry by removing the access required to place explosives or pump gas in the safe.





12 Tactical Tips to Prevent Jackpotting

How Does Jackpotting Happen?

A criminal needs physical access and a rogue device to commit jackpotting – also known as an ATM logical attack. A rogue device doesn't have permission to access a network but can disrupt the network's normal operations and harm or steal information. The criminal uses the rogue device to manipulate settings on the machine to dispense cash until the machine is empty. The cash dispensed is not tied to the balance of any one accountholder.

1 Use Pick-Resistant Keys

Ensure each of your ATMs have one or more specially designed, pick-resistant keys to limit access and thwart universal keys.

2 Secure the BIOS (Basic Input and Output)

Administration of the BIOS must adhere to the following principles:

- During normal operations, configure the BIOS to boot from the primary hard disk only. All other bootable mechanisms should be removed from the boot order to prevent booting from any other unauthorized device.
- Review and test the BIOS updates before deployment
- Protect BIOS operations with unique, non-default passwords
- Wherever possible, use Unified Extensible Firmware Interface (UEFI) Secure Boot to protect against boot vector attacks. UEFI Secure Boot is a security feature within the UEFI firmware that prevents malicious code from taking control during the boot process by verifying the digital signatures of boot components.

3 Establish a Strong Password Policy

All default passwords **must** be changed as per [PCI 4.0 requirement 2.2](#). Other criteria include:

- Unique passwords per ATM and per account, giving maximum protection at each ATM and preventing a chain of attacks
- A least 14 characters long and should not contain more than two consecutive characters from the username
- Complex, containing at least three of the following categories:
 - English uppercase alphabet characters (A-Z)
 - English lowercase alphabet characters (a-z)
 - Base 10 digits (0-9)
 - Non-alphanumeric characters (e.g. !@#\$%)
- Change user and administrator passwords every 90 days (as required by [PCI DSS 4.0 requirement 8.3](#))

BIOS passwords should be highly complex to enhance security. Consult with your ATM vendor for additional solutions for managing BIOS passwords.

4 Implement Communications Encryption

[PCI DSS 4.0 Requirement 4.2.1](#) states that strong cryptography and security protocols to safeguard sensitive cardholder data during transmission are to be used over open, public networks (e.g. internet, wireless technologies, cellular technologies, general packet radio service [GPRS], or satellite communications).

Wireless networks transmitting cardholder data or connected to the cardholder data environment should use industry best practices for implementing strong encryption to secure authentication and data transmission.

SSL and early TLS encryption have been demonstrated to have weaknesses which can be exploited and must not be used as a security control to meet PCI requirements. When it comes to implementing:

- New implementations must not use SSL or early TLS as a security control
- Existing implementations must migrate to a secure TLS version (now 1.2e)
- All use of SSL and early TLS as a security control must be stopped

5 Install and Maintain a Firewall

The ATM firewall must be configured to only allow known authorized incoming and outgoing connections necessary for an ATM environment. Configure the connections by program rather than per port.

6 Remove Unused Services and Applications

Remove any unused services and applications from the system to reduce the attack surface area. A good rule of thumb is: “If you don’t use it, disable it.”

7 Deploy Strong Antivirus Mechanisms

Use antivirus (AV) software to maintain the integrity of your ATM software stack and prevent malicious software compromising your ATM.

An effective white-listing solution will provide online protection – like memory protection, zero-day attacks, and threat alerting – beyond known malware threats.

When using antivirus software, you must:

- Keep software signatures up to date
- Regularly review scan reports/logs to determine if the ATM is infected or not
- Run software weekly on an ATM to detect if known malware exists
- Avoid running software in real-time mode and refrain from excessively frequent log checks, as logs are updated continuously.
- Put the ATM out of service prior to scanning and run during quiet periods
- Update the signature files prior to running the scan

Antivirus software on an ATM should operate in silent mode without pop-up alerts. If the AV software is running in the background, consider process priorities.

If an AV scan reports malware, follow these general incident response procedures:



Procedures may depend on the malware found and other law enforcement input.

8 Establish a Regular Patching Process for Installed Software

Ensure all ATM software is consistently updated with the latest security patches to prevent attackers from exploiting known vulnerabilities. Unpatched weaknesses can enable the installation of malware or unauthorized access to the ATM's software stack. By applying available security patches, these vulnerabilities become non-exploitable, significantly reducing risk.

Staying current with Microsoft security hotfixes is **essential to safeguard the operating system** from known threats. Unaddressed vulnerabilities can serve as entry points for malware or other forms of attack.

[PCI DSS Requirements 6.1 and 6.2](#) emphasize the importance of applying vendor-supplied security patches to protect systems from known exploits. If an ATM operates on an unsupported operating system, necessary security updates may no longer be available, making compliance with these requirements unattainable.

It's critical that ATMs run on a supported operating system. [Industry reports](#) indicate that a significant number of ATMs still operate on outdated platforms. Planning and executing a migration to a supported environment should be prioritized.

Without essential Windows security updates, ATMs may become **vulnerable to viruses**, spyware, and other malicious software—putting cardholder data and business-critical information at serious risk.

9 Harden the Windows OS

The Windows operating system must be hardened to restrict the privileges and behavior of the ATM to only allow necessary self-service functions. When installed in secure mode the software automatically applies over 500 system settings. These configurations strike a balance between the minimum requirements for ATM operation in a standalone environment and industry-recognized system hardening standards.

A locked down OS environment on a standalone ATM based should include:

- Disabling Windows auto-play: Auto-play is a feature of Windows operating systems which allows software to run from removable media as soon as it is detected on a USB, DVD, or CD. Disabling this feature within the operating system will prevent malware being automatically run when it is detected on removable media.
- Establishing locked-down user account – few privileges and no interactive desktop access – for automatically running self-service application functionality
- Implementing a keyboard disabler to block keypresses being interpreted within the locked down account
- Restricting minimal file, folder, and registry permissions
- Applying computer and user policies that restrict functionality required for the ATM application to function correctly and securely

10 Deploy Full Hard Drive Encryption

Full hard disk encryption renders the contents of the hard disk unreadable, **protecting against malware attacks** even when the ATM hard disk is offline (e.g. the ATM is booted from bootable removable media, is removed from the ATM and mounted as a secondary drive, the core is removed from the ATM).

11 Protect Communication Between the ATM Core and the Dispenser

Encrypt the communications between the ATM core and the dispenser to prevent black box attacks. Only commands from the ATM software stack will be authenticated and processed by the dispenser. External attempts to send commands directly to the dispenser will be **flagged as invalid**.

12 Perform an Annual Penetration Test

An external organization should perform the annual simulation tests to find misconfigurations, weaknesses, and vulnerabilities that could be exploited by an attacker. The penetration test should reveal any areas that need to be addressed to **optimally secure** all ATMs from jackpotting attacks.



Alarm and Camera Security Features

Consider these feature enhancements to further ATM security.



Alarm System Sensors:

- **Vibration sensors** detect attempts to tamper with or damage the ATM
- **Tilt sensors** detect unauthorized movement or attempts to move the ATM
- **Pressure switches** trigger an alarm if the ATM's casing is opened or tampered with
- **Temperature and humidity sensors** detect unusual temperature or humidity levels that could indicate tampering or environmental issues
- **Gas detectors** detect the presence of gas leaks, which can be a sign of a potential threat



Alarm Output Devices:

- **Audible alarms** are loud sirens to alert nearby individuals and deter potential attackers
- **Visual alarms** utilize flashing lights to attract attention and deter attackers
- **Fog** cannons release harmless fog to deter attackers and obscure the ATM



Communication Devices:

- **Speech dialers** automatically call pre-programmed numbers (e.g., police, security) to report an alarm
- **SMS/GSM dialers** send text messages to notify security personnel or other contacts



Keys:

- **High-security locks** are unique to each financial institution and deter generic, universal keys that can be easily purchased by criminals.



Software Components:

- **Anti-skimming technology** detects and prevents skimming devices from being installed on the ATM
- **Face recognition and detection** can identify and alert security personnel to suspicious activity



Battery Back-Up

- Ability for 24-hour standby and operate in full alarm mode (e.g., with all sounders running) for at least 30 minutes
- System load will determine the battery capacity needed (this is the amount of power consumed by the ATM alarm system components such as panels, sensors, sounders, etc.)
- Batteries should fully recharge by the alarm panel within 48 hours after full discharge



ATM Video Surveillance

Strategically placed cameras, combined with real-time alerts triggered by security breaches, enable the video surveillance system to immediately notify the monitoring center – allowing for rapid response and investigation. Camera footage should capture ATM transactions as well as surrounding, critical areas (including entrances, corners, and the ATM itself.) Security camera footage is crucial in helping law enforcement understand and appropriately pursue incidents where customer assets are compromised, plus security officers can quickly investigate claims of theft or suspicious behavior.



Features of ATM Security Cameras:

- **High resolution** ensures clear footage for identification and investigation
- **Intelligent motion detection** triggers alerts when suspicious activity is detected
- **Night vision** enables clear visibility even in low-light conditions
- **Large storage capacity** allows for extended recording and storage of footage
- **Facial detection and recognition** detect faces to recognize individuals
- **IoT*-based ATM security solutions** trigger alarms when predefined criteria for tampering ATM removal/shutter sensors, chest door MCS sensors, vibration sensors, motion sensors, thermal sensors, glass break sensors, and smoke sensors are met

The Internet of Things (IoT) refers to a network of physical objects, or "things," embedded with sensors, software, and network connectivity that enable them to collect and exchange data, allowing for remote monitoring, control, and automation.

How Artificial Intelligence is Enhancing ATM Security

Artificial Intelligence (AI) is playing an increasingly vital role in enhancing ATM security and aiding fraud prevention. AI-powered fraud detection systems can analyze real-time transaction data to identify unusual patterns—such as atypical withdrawal amounts or unfamiliar locations—allowing financial institutions to respond proactively before fraud occurs. Beyond transactions, AI can monitor ATM surroundings to **detect abnormal behaviors**, like individuals lingering too long or unusually large groups gathering, which may indicate suspicious activity.

Integrating biometric authentication technologies, such as facial recognition and fingerprint scanning, into ATMs strengthens identity verification. These methods add an **extra layer of protection** beyond traditional PINs and cards, making it significantly harder for unauthorized users to gain access to customer accounts.

AI also enhances physical security. By analyzing video footage and sensor data, it can detect and help prevent physical attacks on ATMs—such as hook and chain methods—before significant damage is done. Additionally, AI-driven tampering detection systems can **continuously monitor unauthorized access** or signs of damage, instantly alerting security personnel for rapid response.

AI is evolving beyond basic data analysis, giving financial institutions a significant advantage to halt ATM fraud while bridging the gap between digital self-service and in-branch banking experiences. These services are expanding beyond basic withdrawals to incorporate buying, selling, and managing cryptocurrencies. QR code technology and mobile banking integrations offer contactless transactions, while cash recycling features deposit and deliver cash in different denominations. AI is being used to enhance ATM security, improve member/customer service, and optimize cash management.

In Summary

Regular ATM security reviews are crucial for financial institutions to stay ahead of evolving threats and maintain customer trust. These reviews should focus on both physical and cyber security, including measures to protect against skimming devices, malware, and system breaches. A thorough review helps ensure the integrity of ATM systems and the security of customer data.

Criminals will always find new ways to target ATMs. As their tactics evolve, so must your defenses. **The best approach is a proactive one**—securing your ATMs with layered security measures that slow down attacks and deter criminals. There's no one-size-fits-all solution, but working closely with law enforcement, ATM providers, and security vendors is key to staying ahead.



The best approach is a proactive one—securing your ATMs with layered security measures that slow down attacks and deter criminals.

About Allied Solutions

Allied Solutions is one of the largest providers of insurance, lending, risk management, and data-driven solutions to financial institutions in North America. Allied Solutions uses technology-based solutions customized to meet the needs of over 6,000 banks, credit unions, finance companies, mortgage servicers, and auto dealers, along with a portfolio of innovative products and services from a wide variety of providers. Allied Solutions is headquartered in Carmel, Indiana and maintains several offices strategically located across the country. Allied Solutions is a wholly owned and independently operated subsidiary of Securian Financial Group.



Learn More



| [Follow Allied on LinkedIn](#)



| [Like Allied on Facebook](#)



| [Read Allied Insights Thought Leadership](#)



| [Subscribe to Allied Insights Newsletters](#)



| [Listen to The Allied Angle on Podbean](#)



Allied Solutions®

GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

alliedsolutions.net

© 2025 Allied Solutions, LLC.

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.

2190-R2-5.25