CUMMINS ALLISON

ATM Security Solutions

Safeguarding your ATMs against physical and cyber attacks

ATMs are attractive targets for criminals, and crimes against them are constantly evolving. In fact, criminals who target ATMs cost the industry billions of dollars every year. To anticipate and combat the threat against ATMs, you need to implement effective and comprehensive security solutions.

While attack approaches vary widely, ATM attacks fall into three main categories:

- Physical device tampering
- Network attacks
- Operating system or application attacks

Physical Security Solutions

The first line of defense has to be implemented at the ATM itself. ATM fraud is by far the greatest threat to ATM security, accounting for more than 90% of the recorded ATM incidents. We offer the following countermeasures for device-level protection:

Anti-skim EMV card reader

Skimming devices can be added to card readers so quickly they can easily go unnoticed. To protect cardholder data and combat skimming attempts, Cummins Allison protects its EMV motorized and DIP card reader with the following anti-skimming technologies:

Jamming
When a skimming device is detected, the card reader generates an electromagnetic field to prevent the skimming device from reading a consumer's card information. The field is designed to interfere with the skimming device operation without affecting the normal operation of the ATM.

Metal detection
A built-in metal detector monitors for a metallic object attached to the bezel. If a skimming device is detected, the ATM is taken out of service until the threat is removed. Once the threat is removed, the ATM returns to service without any interaction, eliminating the need for a service call.

Unique shutter design
A unique design inhibits/prevents the card reader and shutter from being forced open. If an inserted item does not meet the standard bank card width or magnetic features, the card reader rejects the item and returns it to the user.

Unique sensors and bezel design
The physical shape of the card reader and fascia prevents perpetrators from attaching a card skimming device around the ATM card reader or applying a false front. If tampering occurs and the detection sensor is covered or compromised, the ATM is taken out of service.

Dispenser security

Attempts to disconnect the ATM's cash dispenser from the core computer to send unauthorized 'jackpotting' commands are prevented using encryption. If the synchronization between these two is compromised, re-synchronization between the two must take place before a dispense command is recognized.

Safes and locks

We offer a UL 291-certified business-hour or a heavy-duty Level-1 safe. ATMs come standard with an electronic lock or an optional Kaba Mas Cencon lock.

Cummins Allison takes security seriously and offers multiple points of protection using proven technologies to safeguard your ATMs. From physical security solutions to endpoint security, to software maintenance and remote support, we are ready to protect your ATM installations.

Awareness mirror

Help consumers feel more secure when they conduct transactions at your ATM. Awareness mirrors provide your consumers with the broadest viewing range and a greater sense of safety.

PIN pad shield

An ATM keypad shield helps conceal the consumer's hand during PIN entry, providing a simple but effective solution to the challenges of ATM security.

Alarms and cameras

Video cameras and alarms serve as a deterrent in protecting your ATMs. We can work with your current security provider to integrate these devices into your fleet.

No protection is absolute but a combination of awareness and preventative tools will make your ATMs as safe as they can be.

Network and Operating System Solutions

While traditional security measures including firewalls and antivirus software should be installed, maximum data protection requires a more robust solution, such as Cummins Allison's Endpoint Security.

Endpoint Security is a managed service that minimizes the possibility of jackpotting and other malware threats. A software agent is placed on your ATM to continually monitor the security status of your ATMs and reports back to a management server. The server monitors its connected endpoints (ATMs) to deploy policies that block, contain and quarantine potential threats. The service provides the following types of protection:

Access and program control

Access control ensures ATMs are compliant with deployed security policies. A firewall controls the inbound and outbound network traffic, allowing only legitimate, approved programs communicate. Whitelisting allows only approved programs to run and perform tasks. Unapproved applications and untrusted applications are blacklisted, blocked or terminated.

Media encryption and port protection

Encryption software automatically protects all information on the hard drive—including user data, the operating system, temporary files and erased files. Media encryption and port protection secures removable media devices such as USB flash drives, backup hard drives and CDs, and enable restricting or blocking of physical ports.

Ransomware protection

Ransomware protection uses a behavioral analysis engine capable of detecting, blocking, disabling and removing ransomware. It also restores any encrypted data as part of its automated remediation capability.

Zero-day protection

To prevent 'zero-day' attacks, a threat emulation engine is used to identify potentially malicious files, then employs sandboxing techniques to assess the activity in a virtual environment in order to maintain the integrity of the network.

Anti-bot security protection

Bots are malicious, stealthy software that invade your network and enables criminals to control your ATM remotely. Anti-bot software identifies an infected host and shuts down all bot communications from that host, effectively neutralizing the threat.

Full visibility of security events

Should security events occur, incident reports provide actionable information—origin of attack, scope of damage, impact to ATM—to enable a faster and more effective response. Reports can be customized based on your organization's requirements.

Software Maintenance and Remote Support

Availability of your ATM network is vital to your brand. To be sure it performs optimally, it is important to keep its software updated with the latest security patches. We recommend our customers protect their investment with Cummins Allison's Software Maintenance and Remote Support advantage at the time of purchase. This service helps you reduce risks by ensuring you have the latest versions of ATM software and operating system updates.

Get in touch with us to dive deeper and find out how we can help you better protect your ATMs. Contact your local representative, visit **cumminsallison.com** or call **800-786-5528**.

CUMMINS ALLISON

852 Feehanville Drive Mt. Prospect, IL 60056 **T** 800 786 5528 **cumminsallison.com**

Technology innovators and efficiency experts, Cummins Allison transforms the way coin, currency, and checks are counted, sorted and authenticated, and our expanded portfolio includes full-function ATMs. Leading financial, retail and gaming organizations rely on us for the fastest and most accurate solutions in the industry. Our global footprint includes headquarters near Chicago, more than 40 offices in the US and a presence in over 70 countries worldwide. Since 1887, we've been dedicated to quality, reliability and the highest level of customer satisfaction.

023-1995 Rev. A