RBI CONTROL MEASURES MANDATE

GUIDE TO ATM SECURTY AND PROTECTION

Upgrading or replacing your ATMs
to expand India’s financial inclusion

An NCR white paper

RBI ATM CONTROL MEASURES MANDATE: YOUR OPPORTUNITY

In June 2018, the Reserve Bank of India (RBI) notified banks and ATM operators across India that they were required to upgrade or replace their ATM software and hardware.

This mandatory change is due to long-running concerns RBI has had over unsupported operating systems in use on the country's ATMs. An unsupported OS can put customer data and financial institutions at risk of security breaches - and hurt the country's ability to meet its financial inclusion goals.

The mandate is a catalyst for modernizing your ATM estate, future-proofing it against security attacks and providing consumers with an improved experience. Seize the opportunity to differentiate your bank by replacing legacy ATMs with the latest single footprint and multifunction ATMs and software.

Installing new ATMs ensures they're running the latest OS, which will keep you compliant until at least 2025, but can also provide modern features to attract more customers – like touchscreens, intelligent deposit capabilities and contactless transactions.

Every week we hear new reports of attacks on ATMs from around the world. More and more frequently we hear of ways that criminals continue to vary and modify their attacks to attempt to bypass the protections in place. The sophistication of the criminal's tools and methods have also increased. With security built-in from the ground up, NCR offer a number of ATM solutions "designed in" to ensure your ATM channel is more secure than ever before.

Understanding each of the crimes can become complicated and seem overwhelming. When looking at the broader picture each type of crime falls into three general categories.

- **Logical theft of valuable media**
- **Identity theft**
- **Physical theft of valuable media**

In this paper, we will describe the attack techniques that are used, and illustrate how the attacks evolve as an 'arms race' develops between the defenders and the attackers. NCR will also describe how our SelfServ family of ATMs has deployed effective strategies for each category that can be used to win the war in each case.

TABLE OF CONTENTS

LOGICAL THEFT OF VALUABLE MEDIA

Logical theft of valuable media refers to the category of crimes used to steal cash, or other valuable media, from the ATM using methods which do not physically breach the cash enclosure.

This cybercrime makes use of modern technology to exploit ATM features which weren't considered vulnerable at the time of the original ATM design -- and it's the area where the industry is experiencing the greatest rise in number and variety of attacks.

Since 2012 there has been an significant increase in the frequency of these attacks, and successful logical attacks have been executed across the globe. The nature of these crimes allow the attack to occur on a large number of ATMs at once. The outcome of the crime could be the theft of all of the cash in the ATM. This can lead to very significant financial losses in a very short period of time.

Typically, these attacks fall into three major categories:

- **Black box attacks**
- **Malware in the network**
- **Malware installed on the ATM**

In a **black box attack**, the criminal gains access to the dispenser cable inside the ATM. They then bypass the ATM's core processor and connect an electronic device to the cash dispenser. The criminal is then able to send unauthorized commands to dispense cash from the ATM.

A **network malware attack** allows the criminal to intercept data communications between the ATM and host, which they commonly use to capture information or trigger unauthorized dispensing from the ATM.

Your ATM estate can be protected from these attacks, but an up-to-date operating system is required to run the encryption and detection software.

Since 2012 there has been an alarming increase in the frequency of these forms of attacks

For **attacks where malware is installed on the ATM** hard drive, malicious software allows criminals to send commands to the ATM.

There are two major variations of these malware attacks: In a minority of cases, the attack is carried out while the ATM hard drive is online. This is typically done using USB devices with auto play enabled or using a known Windows® administrator password.

The most common logical attack against ATMs, is an offline attack which occurs when an attacker inserts removable media (for example, DVD, CD or USB) into an ATM core and copies malware to the hard drive. Once the ATM is rebooted, the malware can capture customer data, including ATM card numbers, their associated PINs and the account they're associated with.

These attacks can damage a bank's reputation with customers, which can affect the bank for months or even years.

All these attacks can be prevented by:

- Deployment of whitelisting solutions tools. NCR ATMs have a number of solutions built in as standard to combat black box attacks. NCR Media Handling 2.0 devices use encryption as standard. We also offer solutions designed to protect the software installed on the ATM. This is done by ensuring that only authorized code can run. That authorized code or memory cannot be tampered with or hijacked.
- Encrypting the ATM hard disk. This makes the hard disk unreadable when offline. When it is unreadable, attackers cannot copy malware onto the hard disk.
- Locking down the BIOS. This prevents the ATM from booting to removable media. When an attacker inserts removable media into the ATM core and restarts the ATM, the ATM will not boot to that device. The ATM will start as normal.
- Encrypting the ATM hard disk. NCR Secure Hard Disk Encryption is the most comprehensive protection against offline attacks on ATMs.

These solutions:

- Protect against offline malware attacks
- Prevent malware being copied onto the hard disk when the ATM is booted from removable media
- Prevent malware being copied onto the hard disk when the ATM hard disk is removed and mounted as a secondary drive
- Ensure the content of the hard disk is encrypted and unreadable when it is removed from the ATM core, when the core is removed from the ATM, or when network connectivity is compromised

In addition to preventing offline attacks, NCR Secure Hard Disk Encryption also prevents reverse engineering of the deployed software stack. The solution prevents dispenser encryption keys being copied from the hard drive when it is offline. This will provide an additional layer of protection from black box attacks.

PROTECTION FROM LOGICAL ATTACKS IS ONLY POSSIBLE THROUGH THE COMPLETE DEPLOYMENT OF A LAYERED AND COMPREHENSIVE SET OF SECURITY GUIDELINES. THESE INCLUDE:

Secure the ATM BIOS to only allow boot from the primary hard disk. BIOS editing must be password protected.	Deploy a network authentication based hard disk encryption solution such as NCR's Secure Hard Disk Encryption solution.
Establish an adequate operational password policy for all passwords. A single password for every ATM is not secure.	Remove unused services and applications. Any code is a source of vulnerability, so minimize it.
Implement communications encryption (TLS encryption or VPN). This should be considered as mandatory if you are using public wide area networks.	Deploy an effective anti-virus mechanism. NCR recommends active whitelisting applications such as NCR's Solidcore Suite.
Establish a patching process for Operating System Patches.	Remotely and securely control passwords with enhanced permissions.
Establish a regular patching process for ALL software installed.	Ensure there are protected communications to the dispenser of the ATM.
Establish a firewall. This also should be considered as mandatory if the ATMs are on a public wide area network.	Use Remote Software Distribution. This helps enable some of the earlier security requirements.
Define different accounts for different user privileges.	Perform a Penetration Test of your ATM production environment annually.
Ensure the application runs in a locked down account with minimum privileges required.	Consider the physical environment of ATM deployment.
Disable Windows Auto-Play.	

An additional, but critical layer of the solution strategy comes with the deployment of enterprise fraud detection solutions. This layer provides the financial institution with the ability to track and monitor transactions throughout all of their channels. The fraud detection solution will provide the ability to note abnormal transaction patterns. This can include frequency of transactions, location of transactions by geography and by merchant.

IDENTITY THEFT

Identity theft at ATMs are typically hardware attacks, and refers to crimes that capture data used by consumers to authenticate themselves at a self-service terminal.

The most frequent attack types in this category include card skimming, card trapping, and card sniffing.

A card skimming attack is the unauthorized capture of magnetic stripe information. It's achieved by modifying the hardware or software of a payment device, or through the use of a separate card reader, and is often accompanied with the covert capture of customer PIN data. Armed with this information, fraudsters can create dummy cards and raid the customer's account.

The devices used in card skimming attacks employ some form of electronic device to read and capture data from the card's magnetic stripe during the ATM transaction.

The most common forms of card skimmers are:

- **Bezel Mounted Card Skimmers**: These are devices that are made to fit over the existing bezel of the ATM. They appear to look like the authorized bezel.
- **Insert Skimmers:** Are small electronic devices, designed to fit inside the card reader. Due to the nature of their size Insert Skimmers are nearly impossible for the layman to detect.

Card skimming remains by far the most frequent form of ATM scam, and currently accounts for nearly 95% of all losses from ATM attacks. Card skimming is difficult to guard against. As long as the magnetic stripe remains on the card, and the card is passed through any device that reads the magnetic stripe data, there will be the risk of card skimming.

These forms of card skimming can be effectively prevented through the deployment of comprehensive anti-skimming solutions.

But for every security iteration ATM manufacturers develop to combat card skimmers, the criminals aren't far behind.

NCR's strategy to card skimming solutions takes a different approach to this challenge. Effective anti-skimming must contain the ability to both detect the presence of a skimmer, attempt to disable the skimmer and provide notification to the ATM operator that skimming is occurring at that ATM. All of these components are included in NCR Skimming Protection Solution (SPS).

An enhanced flush card reader is the first line of defense against ATM card skimmers, and makes it easier for consumers to identify suspicious devices on the ATM. The enhanced card reader is deep insert resistant, and features encrypted USB communications to further prevent skimming. SPS provides sophisticated detection allowing the device to identify when any item is placed in or around the card bezel. On motorized card readers, NCR provides jamming capabilities to effectively disable the skimmer's ability to capture the card information.

SPS is built with a field programmable framework. This allows us the ability to enhance functionality should criminals modify their attacks. SPS can also be configured to be highly integrated into the ATM monitoring system, allowing ATM operators to receive up to 16 different alerts and notifications. With this level of detail, the ATM operator can determine how they respond to the attack including having the option to take the ATM out of service.

The first line of defense against skimming devices on an NCR ATM is in the **design.**

Eavesdropping Attacks: In this attack, a hole is made in the ATM or access gained to the top box of the ATM. Eavesdropping attacks can be prevented by retrofitting existing ATMs with physical barriers around the internal card reader. NCR has an anti-eavesdropping kit that offers an easy and inexpensive protective measure. The latest SelfServ ATMs have no card orientation window which removes vulnerability to drilling in to the ATM. Furthermore, NCR is working closely with our card reader manufacturers on new designs that add further protection. NCR's Skimming Protection Solution also provides enhanced protection around the card bezel in the form of drill plates. This would make it more difficult for the criminal to cut a hole in the ATM in order to place an eavesdropping device on the card reader.

Network Sniffing Attack: With this approach the criminals attempt to capture the cardholder information as it is being sent from the ATM to the ATM switch or host. This is done by attaching a device onto the network connection cables. There are several layers to the defence strategy to protect against network sniffing attacks.

First, the easiest and immediate defence would be to add a physical barrier to prevent any unauthorized access to the network cables. This can be by shielding the wires in a conduit, or behind the wall. More sophisticated solutions would be to deploy secure communication connections. NCR recommends the implementation of TLS encryption. Encrypted wireless communication can also be deployed in addition to the TLS to provide additional protection against this form of attack.

The following table represents a summary of the attack threats in this area, and the recommended solutions to protect NCR ATMs.

SKIMMING CATEGORY	DESCRIPTION	RECOMMENDED SOLUTIONS
Bezel Overlay	Manufactured overlay containing a skimmer which fits a specific ATM model	SPS with Skimmer Detect and Alert Monitoring
Bezel Insert	Manufactured insert containing a skimmer which fits a specific ATM model	SPS with Skimmer Detect and Alert Monitoring
Card Read Tap—Destructive (Eavesdropping)	Attacks that penetrate the ATM fascia or cabinet with the intention of providing direct access to the card reader	SPS with Skimmer Detect and Alert Monitoring, plus Anti-Eavesdropping Kit
Card Read Tap—Non-Destructive	Attacks that involve opening the ATM cabinet with the intention of providing direct access to the card reader	ATM location security, appropriate cabinet locks, encrypted USB
Differential Skimming (Stereo Skimming)	Using twin read heads connected in differential mode to negate the effects of a jamming signal	SPS with Skimmer Detect and Alert Monitoring
Deep Insert Skimmer	A device placed inside the card reader using the card slot as the entry point	Card reader device detection firmware, third party anti-insert kits
Sabotage	Any attempt to disable any anti-skimming technology	SPS with Skimmer Detect and Alert Monitoring
Shimming	Capture of chip card data with the intent to produce a cloned mag stripe card	Transaction Authorisation as per EMV
Network Sniffing	Capture of card data via sniffing of network communications to the host	Communications Encryption TLS 1.2
Malware Sniffing	Capture of card data via malicious software installed on the ATM hard disk	Secure Hard Disk Encryption

PHYSICAL THEFT

Physical theft of valuable media—the category of crimes that are used to steal cash or other valuable media, from the ATM using methods which physically breach the cash enclosure. This category includes all of the traditional robbery techniques that can be used to open a safe, and includes emerging trends of using explosives.

These crimes continue to a major problem for ATM operators. In the last year, Indian news media has featured several stories about the wide availability on the internet of "how to" guides for ATM hackers.

The main categories of these physical attacks are:

- Explosions to physically breach the safe. Traditionally this was done in certain regions where there was easy access to solid explosives, such as dynamite. More recently we have seen an increase in the use of gas explosives. This has led to these forms of attacks occurring in more areas of the world.
- Cutting the safe by some means of brute force. This can be done using torches or grinders.
- Ram Raid—instances where the ATM is physically removed from its installation environment.

Key protective strategies center around ensuring that ATM operators choose the correct safe based on the threat environment. NCR offers a full line of CEN safes, with CEN 1 as the minimum safe level available. Additionally, customers should consider the use of NCR GasEx resistant safes to prevent against gas explosive attacks. Further defences from physical attacks can be added through deployment of a wide variety of third party solutions.

These solutions include:

Cash degradation solutions such as ink staining or glue solutions that will make the cash unusable if the ATM cassette is breached.

Gas detection/neutralization solutions can be installed to detect the presence of gas used as part of an explosive attack. These devices can be configured to trigger alarms, smoke, sirens, or other notifications. Gas neutralization will counteract the presence of an explosive gas to prevent an explosion from occurring.

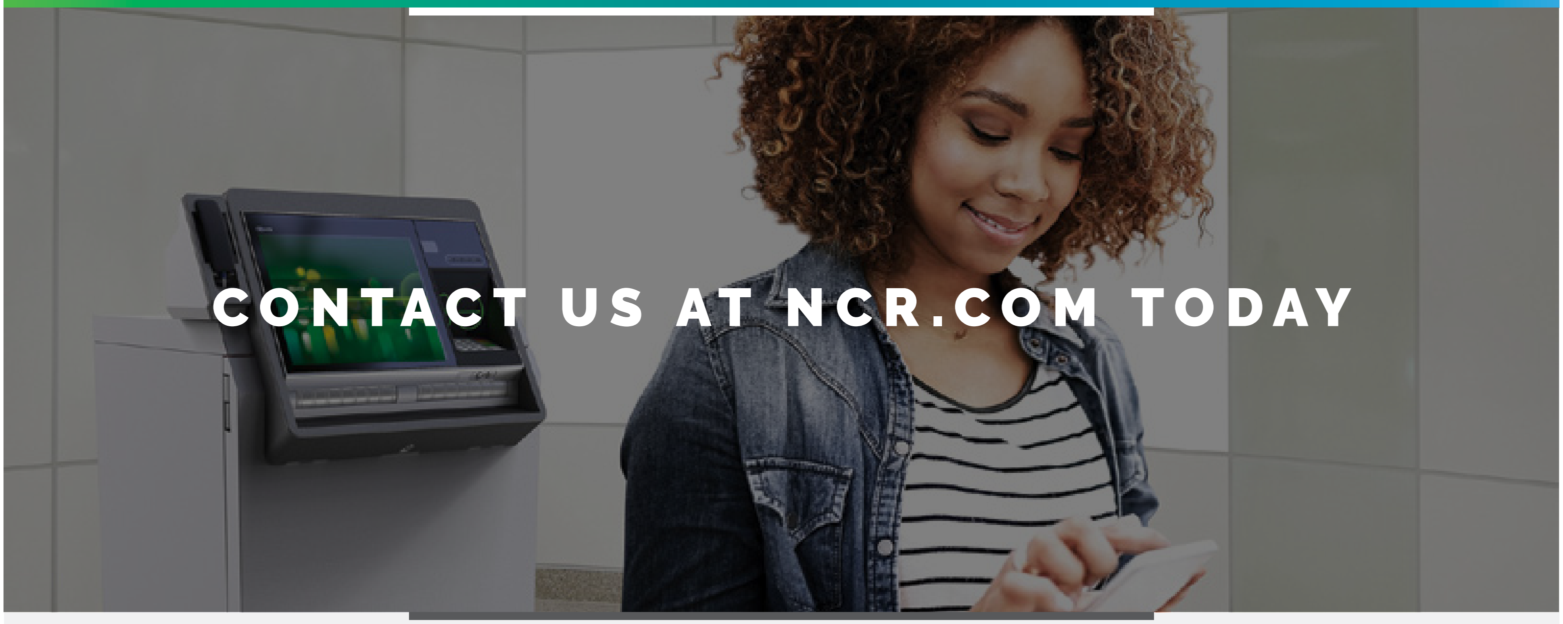
GPS devices and ATM trackers can be installed to both notify when motion is detected on an ATM, and the location of the ATM itself can be monitored.

CONCLUSION

Updating or replacing your ATM estate isn't a choice for many of India's banks and ATM operators. The possibility of RBI imposing penalties on non-compliant operators is too great, and India's push for financial inclusion is too important.

What you can choose is how to implement these upgrades. For some, a phased operating system change from WindowsXP to Windows7 to Windows10 might be the best path. For others, changing the physical hardware while updating the obsolete software might be the strategy that provides greater differentiation and drives loyalty.

NCR's family of ATMs has been designed to help banks and white-label ATM operators deal with the threats to their ATM investments and operations.



WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Ga., with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

 17FIN4425-XX-J-0917 ncr.com