# ALIGNING TO BEST PRACTICES ON ATM CASH OUT ATTACKS

An NCR white paper
September 2018

NCR

SECURE

## OVERVIEW

Security attacks are a real threat to the ATM industry. The traditional attack vectors remain a significant and material threat to ATM operators. Even with some regional variations in frequency ATM crime continues to rise and expand into nearly every global region. Since 2014, the ATM industry has faced a major and growing trend of logical attacks leading to the "jackpotting" of cash from ATMs.

Logical attacks involve the use of electronic devices and/or malware as a way of achieving an unauthorized dispense of cash or stealing card data from an ATM. One of our customers reported that his organization lost more money in one day to a logical attack than they had experienced from any other attack in a whole year. This is a significant data point because it indicates the scale of these attacks, which have now been seen in all geographic regions. Logical attacks have now been seen in all geographic regions.

The number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches, according to the 2017 Data Breach Year-End Review released by the Identity Theft Resource Center® (ITRC) and CyberScout.

Data acquired through these data breaches can be used to create counterfeit cards that can be used at an ATM to obtain cash illicitly. These are being referred to as "cash out" attacks.

Cash out attacks aren't skimming, cash trapping, dispenser fraud, or malware attacks – and they don't require the hacker to breach ATM-level infrastructure.

Data stolen from the bank host, retailer system, SMB online, or other sources could potentially include: card data, account information, PIN or other passwords, addresses or other personally identifiable information.

When criminals use this data to create counterfeit or cloned cards, they can use the cards to withdraw cash at an ATM or use them in "card not present" transactions.

For more information, visit ncr.com, or email financial@ncr.com.

# ALIGNING TO NEW BEST PRACTICE GUIDELINES

In response to these attacks, several groups have provided best practice guidance. To help ATM operators understand their options for implementing these recommendations, NCR offers the following broad suggestions, and recommendations for specific ATM units.

## FBI BEST PRACTICE RECOMMENDATIONS

| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Implement separation of duties or dual authorization procedures for account balance or withdrawal increases above a specified threshold. | Financial institutions should discuss this with their host or processor. |
| Implement application whitelisting to block the execution of malware. | NCR recommends the use of whitelisting solutions (NCR Secure Solidcore Suite) for maintaining software integrity as well as adherence to PCI compliance requirements.<br>These are included in our Security Requirements to Help Protect Against Logical Attacks whitepaper.<br>NCR also offers this capability as a fully managed service – NCR Endpoint Security service. |
| Block execution of files from TEMP directories, from which most phishing malware attempts to execute. | NCR recommends this as part of overall IT practices and as part of our Security Requirements to Help Protect Against Logical Attacks. NCR's Endpoint Security solution can help address this. NCR Secure Solidcore Suite and Hard Disk Encryption will mitigate the risks associated with malware insertion at the ATM. |
| Monitor, audit and limit administrator and business critical accounts with the required access and authority to modify the account attributes mentioned above. | NCR recommends this as part of overall IT practices and as part of our Security Requirements to Help Protect Against Logical Attacks whitepaper. |
| Monitor for remote network protocols and administrative tools used to pivot back into the network or conduct for post exploitation of a network, such as PowerShell, Cobalt Strike and Team Viewer. | Configure an IDS system to monitor all traffic and alert on abnormal behavior.<br>Keep your firewall up to date and configure only to allow known application traffic inward and outward. |
| Monitor for SSL or TLS traffic over non-standard ports. | Configure an IDS system to monitor all traffic and alert on abnormal behavior.<br>Keep your firewall up to date and configure only to allow known application traffic inward and outward. |
| Scrutinize attachments and website hyperlinks contained in emails, and do not open attachments included in unsolicited emails. | Work closely with your internal IT department and security experts with your host processer for broader protection approached. Configure an IDS system to monitor all traffic and alert on abnormal behavior.<br>Keep your firewall up to date and configure only to allow known application traffic inward and outward.<br>Implement a security policy that define allowable behavior within email and web traffic. Educate employees on industry security best practices. e.g. recognizing spam and phishing emails. |

| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Implement an update and patch management cycle. | NCR recommends a formal patch management program to ensure consistent and holistic updates occur at the ATM level. NCR offers this as a formal, Managed Service program through our Software Distribution service offer. The same approach must be enabled with your host processor. |
| Implement strong password requirements and two factor authentication using a physical or digital token when possible for local administrators and business critical roles to inhibit lateral movement. | NCR recommends this as part of overall IT practices and as part of our Security Requirements to Help Protect Against Logical Attacks. NCR can assist with this effort through our formal Remote BIOS Management and Windows Operating System Password Management services. This same practice recommendation should be implemented in all IT infrastructure. |
| Install and regularly update anti-virus or anti-malware software on hosts. | For ATM/ITMs NCR recommends the use of a whitelisting solution (NCR Secure Solidcore Suite or our managed Endpoint Security service) and an Anti-Virus solution, such as NCR's Anti-Virus managed service.<br>This same practice recommendation should be implemented in all IT infrastructure. |
| Implement an incident management system, and prepare an incident response plan for rapid deployment in case of a cyber intrusion. | NCR recommends implementing a real-time, transaction-level monitoring and alerting solution such as INETCO Insight so that transaction incidents can be detected, logged and managed in an incident management system. |
| Update software for ATMs regularly and maintain awareness of security incidents associated with similar ATMs. | NCR strongly recommends that all ATM operators stay current with all software, firmware, and operating system patches. NCR can assist with this through our fully managed Software Distribution service.<br>This practice should be enabled for both ATM networks as well as all other IT infrastructure |

| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Identify areas in systems that disarm alerts, and determine best practices when tampered with. | Implement a Privileged User Management system that monitors changes to configurations and can alert when specific system parameters are tampered with. |
| Implement chip and PIN procedures for debit cards to restrict criminals from using store purchased gift cards as fake debit cards. | The use of EMV and chip-only cards with the elimination of fall back to mag stripe will greatly reduce the risk of counterfeit cards being used at the ATM. |
| Upgrade PowerShell to new versions with enhanced logging features, and centralize logs to detect usage of commonly used malware-related PowerShell commands. | We recommend removing PowerShell if it is isn't required. If required, minimize usage to only allow usage in constrained language mode. |
| Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers. | NCR recommends this as part of overall IT practices and as part of our Security Requirements to Help Protect Against Logical Attacks whitepaper. For ATMs, NCR's Software Distribution service will track, maintain and update the ATM OS and Applications. |

## BANKERS ELECTRONIC CRIMES TASK FORCE / CSBS BEST PRACTICES

| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Know what the bank has – a risk assessment is crucial.<br>• How are the ATMs networked?<br>• What security, both physical and logical, is in place?<br>• Who has access to ATMs (employees, ATM vendors, other service personnel)? | NCR can provide a general risk assessment for your ATM deployment and configuration. Please contact us for more information. |
| Develop detailed data flow diagrams and network topology diagrams to understand the connectivity types.<br>• How are the ATMs connected to the network?<br>• Segregated?<br>• Behind a firewall?<br>• How are the ATMs connected to the switch or processing hub? | Perform a threat model and network mapping of your ATM and all IT enterprise networks to identify all entry points and weaknesses. These can then be mitigated accordingly. |
| Identify bank roles and responsibility should ATM Jackpotting occur through the bank's ATMs.<br>• Has the bank's environment been defined/documented?<br>• Have all contracts related the bank's ATM arrangements been reviewed? | Have a defined incidence response plan in place for fraud and security incidents. |
| Identify third party risk<br>• Who drives the bank's ATMs? Who has access to service them?<br>• What controls does the bank's ATM service provider have in place?<br>• What controls does the bank's ATM driver have in place?<br>• What security controls are in place for:<br>• Unusual volume activity,<br>• Unusual dollar amounts, and<br>• Unusual activity during non-peak times? | Follow best practices for assessing your third-party relationships. NCR recommends implementing a real-time, transaction-level monitoring solution such as INETCO Insight that is able to detect and alert on unusual volume, amount, time, and location anomalies. |

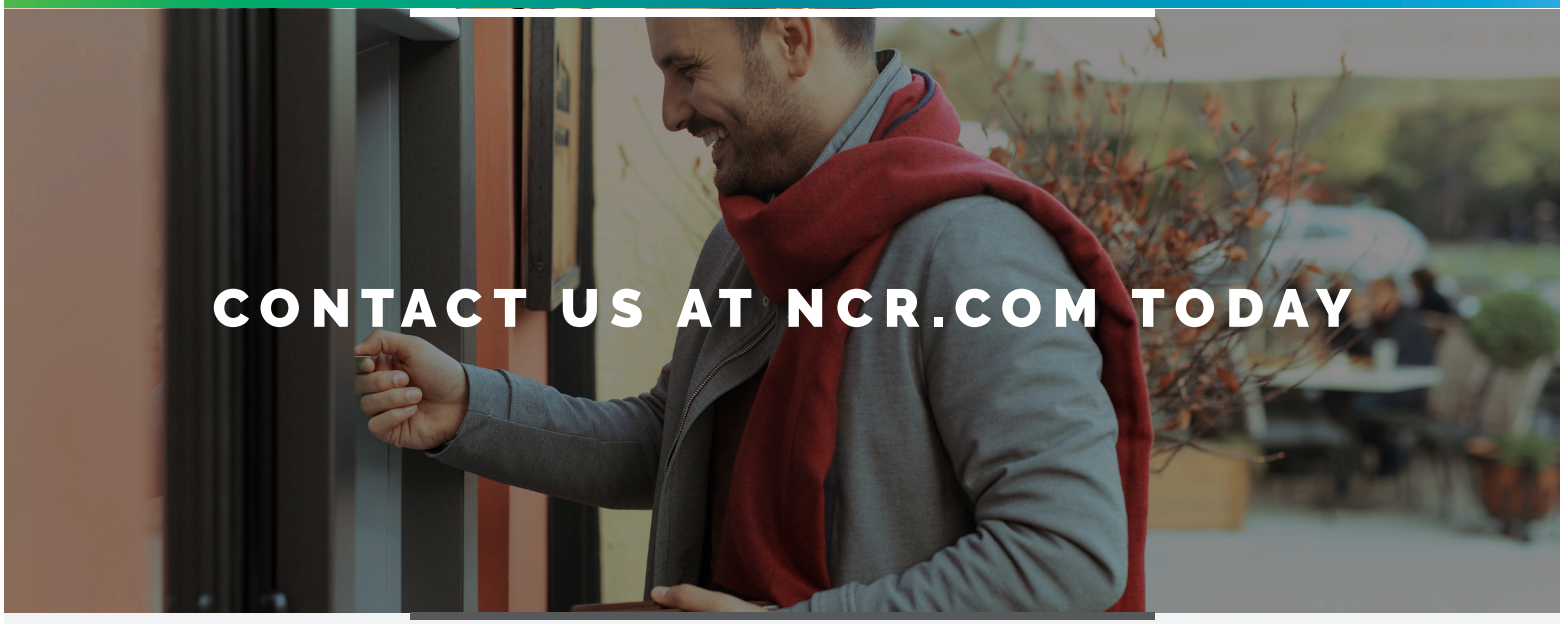
| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Is software support (for patching vulnerabilities) evaluated, regardless of whose responsibility it is?<br>• Are end-of-life software assessments performed?<br>• Has Windows XP been replaced? | All ATM operators must have a plan for migration to Windows 10 to remain on a supported operating system. Contact NCR for more details on our Windows 10 migration programs. Maintaining a fully supported operating system is included as part of Security Requirements to Help Protect Against Logical Attacks whitepaper<br>NCR provides a fully managed service which maintains a program for the updating and patching of ATM operating systems and applications. |
| Control physical access.<br>• Are only those with a need able to physically access the bank's ATMs?<br>• Do you regularly review who has access to the bank's ATMs (employees and third parties)?<br>• If ATMs are inside the institution, are they behind a locked door? | NCR recommends that you control physical access to ATMs based on need and role. |
| Consider making ATM cabinets more secure.<br>• Have default or master style keys and locks been changed to unique sets?<br>• Has adding cabinet alarms been considered? | NCR provides the option for upgraded top box lock keys, as well as unique ATM keys. |
| Segment ATMs from the rest of the bank's network via firewall, VLANs, etc.<br>• Have you used logical security to help reduce an adversaries' movement? | Configuration for this is recommended and is currently part of NCR Security for APTRA. More information can be obtained by contacting NCR. |
| Ensure ATM hard drives are encrypted, BIOS systems are read only or password protected and that boot devices in BIOS are internal only (primary HHD, no CD or USB boot allowed). | This should be considered a mandatory deployment for the prevention of malware insertion on the ATM. NCR provides both software and fully managed solutions for remote enablement of BIOS passwords and setting with NCR Secure Remote BIOS Update, and disc encryption with NCR Secure Hard Disk Encryption. |
| Ensure that a strict password policy is in place.<br>• Is it required that default passwords be changed?<br>• Are complex passwords used? | Follow NCR's guidance on password polices for ATMs. NCR offers password management for both the BIOS as well as the Windows Operating System. |
| Maintain regular cyber hygiene practices consistent with other bank systems.<br>• Are end of life software packages replaced / updated?<br>• Are good patching policies followed?<br>• If managed by a third party, are their practices reviewed?<br>• Has AutoPlay within Windows been disabled?<br>• Is the use of external devices (flash drives, memory cards, CD ROM, etc.) limited?<br>• Is installation of unnecessary software (e.g. Acrobat Reader, RDP, etc.) prohibited? | Follow industry best-practice. NCR Software and fully managed solution can help achieve the proper level of cyber hygiene. |
| Ensure proper training of staff members.<br>• Is social engineering training done regularly, since adversaries have to get either physical or logical access to launch an attack? | NCR recommends that all staff receive ongoing training on how to recognize and detect messages and activities that can lead to exposure to these types of attacks. |

| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Utilize resources to regularly receive information regarding new threats and schemes to reduce the risks of ATM Jackpotting schemes (FS-ISAC and ATM vendor). | In addition to these resources we strongly recommend that you enroll in the ATM security alerts. These messages are sent when NCR is notified of new attack vectors, geographic expansion of attacks or other significant security and fraud issues.<br>Enrollment is free of charge at *http://response.ncr.com/security-alerts* |
| Evaluate other ATMs controls.<br>• Are skimming devices detected?<br>• Have malware controls been installed? | NCR can provide a general risk assessment for your ATM deployment and configuration. Please contact us for more information. |
| Use dedicated computers that are not connected to (or that are segmented from) the bank's network to access ATM consoles / ATM portals.<br>• Have the computers been configured to prevent email access, web access (other than to the ATM portal) and use of USB drives (unless needed)? | Our Security Requirements to Help Protect Against Logical Attacks whitepaper recommends disabling remote desktop access and software delivery utilized for patching, installation and configuration. |
| Establish a known clean baseline for all ATM hardware that can be used as a measurement to determine any deviations.<br>• What is usual volume activity for all time periods?<br>• What are typical patterns of dollar amount withdrawals and frequency?<br>• What is usual activity during non-peak times?<br>• Is the cash level monitored and is that the only indicator of compromise for attacks that do not use cards / accounts?<br>• Is the volume/dollar activity monitored across the bank's ATM estate?<br>• Is the volume/dollar activity monitored across the bank's card base? | NCR recommends implementing a real-time, transaction-level monitoring solution such as INETCO Insight which is able to detect deviations associated with volume, value, and frequency and location. The rules should be flexible and extensible to cater for variations and features. Sample rules may include:<br>• X number of foreign transactions within Y mins<br>• X number of transactions by foreign cards in the last Y mins<br>• X or more bank cards carrying out withdrawals on the same foreign terminal within Y minutes.<br>• X number of consecutives magnetic stripe transactions (instead of chip) from a specific ATM<br>• Cash withdrawal observed on an ATM/ISO link with no matching host/database transaction |
| Monitor system hardware and software for any discreet or overt changes to the operating system, BIOS, boot configuration, or hardware configuration. | NCR software and fully managed Endpoint Security and Remote BIOS Management services solution can assist in meeting this recommendation. |
| Receive alerts if the USB port is utilized. | NCR's software and fully managed services based on Solidcore Suite for APTRA & NCR HDE can protect against unauthorized USB Storage devices being inserted. |
| Limit administrator rights, and receive alerts if login occurs. | Limit administrator rights as part of your complete IT practice. |
| Implement real time monitoring of software activity on ATMs to detect unusual activity. | NCR's software and/or fully managed Endpoint Security service based on Solidcore Suite for APTRA can assist in meeting this recommendation. |
| Establish processes to regularly inspect units physically for unauthorized access or tampering.<br>• Has a list of indicators of physical tampering been created?<br>• Has the frequency of inspections been specified? | NCR recommends frequent physical inspection for all ATMs. This is even a higher priority for unattended ATMs. |

| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Act immediately and with urgency when anomalies are detected. | Implement an incident response policy. |
| Ensure that the institution has an appropriately written (and tested) Incident Response Plan—and follow it.<br>a. Does it ensure that the attack vector is identified and mitigated?<br>b. Are the bank's device models and system types documented?<br>a. If a skimmer or black box is found on an ATM, how many other ATMs of that brand and type does the bank have? Where are they?<br>b. Are all other ATMs of the same model / family reviewed to ensure no additional compromises?<br>Rd3. Contact appropriate law enforcement, legal counsel, and insurance representatives immediately.<br>Rd4. Consider shutting down the ATM network and/or turning off all ATM cards if widespread fraudulent withdrawals are occurring. | Implement an incident response policy. |
| Have a contract for forensics services.<br>Rr2. Ensure clean-state backups are readily available and tested.<br>Rr3. Perform a lessons-learned debrief after a full and complete recovery.<br>Rr4. Document how to prevent this in the future for the same type of event or for different locations. | NCR recommends this as part of your overall IT servicing deployment. |

## ADDITIONAL BEST PRACTICE

| BEST PRACTICE RECOMMENDATION | NCR SUGGESTION |
|---|---|
| Detect "man-in-the middle" Attacks in the payment environment: Monitor the transaction journey from ingress to egress and detect when the transaction has been intercepted or tampered with. | Advanced Persistent Threats in the payment environment may make use of malware on the transaction switch or rogue switches that either alter transaction values, or intercept and approves transactions without the transaction ever going to the authorization host. Monitoring the journey of the transaction and ensuring that the transaction request goes to the intended authorization host, untampered while the transaction traverses several network and application elements, will eliminate man-in-the-middle attacks. NCR recommends INETCO Insight. |



# CONTACT US AT NCR.COM TODAY

## 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.



NCR

SECURE