# NCR ATM SECURITY UPDATE

**Date: January 26, 2018** **Incident No: 2018-03** **REV: #1**

# Warning of Logical (Jackpot) Attacks on ATMs in the United States

## Summary:

NCR has received reports from the U.S Secret Service and other sources of logical (jackpot) attacks on ATMs in the US. While at present these appear focused on non-NCR ATMs, logical attacks are an industry-wide issue. This represents the first confirmed cases of losses due to logical attacks in the US. This should be treated by all ATM deployers as a call to action to take appropriate steps to protect their ATMs against these forms of attack and mitigate any consequences.

## Specific Guidance and Recommendations

The most common forms of logical attack against ATMs are "Black Box" and "Offline Malware".

- Configuring Dispenser Protection on your NCR ATMs to Level 3, and ensuring that the dispenser's driver software is patched with the latest updates, are important protections to mitigate the impact of Black Box attacks.
- Protections for Offline Malware include deploying NCR Secure Hard Drive Encryption and/or locking the ATM BIOS configuration and protecting the configuration with a password. This can be enabled by using NCR Secure Remote BIOS Update
- Further protection from Online Malware attacks can be achieved by deploying a whitelisting solution such as NCR Solidcore Suite for APTRA.

## General Guidance and Recommendations

The impacts of logical attacks can be mitigated by following the guidelines within NCR best practice recommendations and guidelines. Customers who currently do not have the security controls in their own environments that are described within **NCR Logical Security: Security Requirements to Help Protect Against Logical Attacks** are advised to review the document and apply the security controls as quickly as possible. These guidelines are provided within the **NCR Logical Attack Protection Whitepaper**. Protection and mitigation are functions not only of ATM provider updates,

but also the deployer's own security environment.

Customers who would like additional guidance as to their current state of security deployment and how it aligns with NCR's best practices are encouraged to sign up for the **ATM Security Assessment**.

## Informational Webinar:

This development, as well as recent announcements which highlighted new vulnerabilities in PC processing chips, as well as new organized criminal activities. Join experts from NCR Security for an informational and interactive webinar to learn more about these risks and the steps that you can take to proactively protect your ATMs from logical attacks. Click below to register for one of the upcoming webinars:

**February 6th: 10:00 AM (US Eastern Time)**
**February 14th: 12:00 PM (US Eastern Time)**
**February 22nd -2:00 PM (US Eastern Time)**

Please contact your NCR Account Manager if you have any questions or need additional information.

## Contacts

ATM Crime Reporting: **global.security@ncr.com**
Self-Service Security Solutions and Best Practice: **NCRSelf-Service.security@ncr.com**
Further information on this alert please contact **Owen Wild**
Please refer any media inquiries or questions to **Aaron Gould**