

NCR SECURITY UPDATE

DATE: August 17, 2018

INCIDENT NO: 2018-08

REV: #1

FBI Warning on Unlimited Cash Out Attacks in the U.S.

Summary

NCR is aware of warnings being issued to financial institutions in the U.S around the potential of criminals planning to conduct an attack where cloned or counterfeit cards are used to obtain cash from ATMs. Unlimited operations is not a new type of fraud and we have alerted our customers regarding this since 2013.

These “cash out” attacks do not involve any breach of the ATM-level infrastructure. It is not a skimming, cash trapping, dispenser fraud or malware attack.

In these attacks, criminals have obtained consumer information from a bank host, retailer system, SMB online, etc. The data obtained can potentially include card data, account information, PIN, other passwords, addresses, etc. Counterfeit or cloned cards have been manufactured by the criminals. The criminals use these cards to redeem cash at the ATM. The criminals may also use these cards in “Card Not Present” transactions.

This attack is different from the ATM Malware Attacks that we have previously communicated, and the ATM anti-malware solutions are not relevant to this attack.

Suggestions for consideration:

- Follow the guidance that was communicated by the FBI
- Contact your ATM switch provider to get advice on how to protect ATM transactions against fraudulent behavior
- Disable PIN change functionality at your ATMs and monitor PIN change or Non-financial event changes via your IVR/CSR environment

NCR SECURITY UPDATE

- Consider some general security and fraud protection best practice suggestions:
 - Review your infrastructure security plan and ensure it's working as expected to prevent intrusive attacks
 - Consider conducting a forensic review of your infrastructure security measures and remediate gaps immediately
 - Ensure you are monitoring your other channels in case this announcement is an attempt at misdirection of resources
 - If possible, watch the velocity of transactions of the overall ATM network for spikes in the number of withdrawals or overall activity
- Check your ATM withdrawal limit for non-bank cards, i.e. debit cards not issued by your institution.
- Continue to move forward with other security measures such as Infrastructure security, endpoint security, encrypted communication, hard disk encryption and BIOS security
- If you are currently running a Fraud Protection Solution (such as Fractals) there are some steps that you may be able to take to monitor the transactions for anomalous behavior – but there are limitations to this. Please contact your Fraud protection provider or NCR, if you are using Fractals
- Watch for any shift of this into the digital channel - so institutions should be on the lookout for non-financial account changes such as phone, address, etc.
- Full deployment of EMV, using Chip-only transactions can reduce the risk of use from counterfeit cards

NCR ATM Security Summit:

NCR will be holding our 6th Annual NCR ATM Security Summit on Oct 8, 2018. The event, which will occur in London prior to the RBR Cyber and Security conference, is an opportunity to present and discuss the critical topics relating to ATM Security with your peers. [View our online information for more details and to register for this event.](#)

Contacts

© 2018 NCR Corporation. All rights reserved.



NCR SECURITY UPDATE

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](#)