NCR ATM SECURITY UPDATE

DATE: July 9, 2018 **INCIDENT NO:** 2018-06 **REV:** 1

Transaction Reversal Fraud - Global

Summary

NCR is receiving reports from multiple global locations of a specific form of Transaction Reversal Fraud (TRF).

TRF is a fraud method of obtaining cash from the ATM without the account used to initiate the transaction from being debited. This is typically accomplished by the criminal inducing a fault at the ATM during the cash dispense operation such that the host application software logic will reverse the transaction (i.e. not debit the account), although the ATM will dispense the cash and the criminal will remove it from the ATM.

Criminals will typically use anonymous accounts for this fraud to avoid detection, often using prepaid cards or stolen or skimmed cards.

This particular form of TRF has been reported in the United Kingdom, Ukraine, and Canada to date. The typical ATM models attacked are Through-The-Wall (TTW) ATMs, such as the NCR 6634 and 6625.

Fraud Description:

The M.O. in the recent reports uses a technique that causes a fault at the ATM card reader during the cash dispense transaction. A card and PIN are correctly entered into the ATM, and a cash withdrawal is requested. While the transaction is being authorized at the host, the ATM will pre-position the bills behind the dispenser shutter, ready to dispense. The card is ejected, and

rather than take the card as per a normal transaction, the criminal leaves the card in the slot. The ATM transaction will timeout, and the card reader will attempt to capture the card. At this point, the criminal will hold onto the card preventing it from being captured. This results in the ATM reporting a card jam, and because no cash has been dispensed, the host software will reverse the transaction. Now the criminal will force open the dispenser shutter and remove the cash before the ATM has an opportunity to put the cash into the dispenser reject bin.

This crime depends on precise timing and we have reliable reports that a tool is used to hold the card in the reader, allowing the criminal to concentrate on removing the cash from the dispenser.

Note 1: a variation on this M.O. could be to allow the card to be captured by the ATM. This has not been observed, but deployers should be aware of the possibility.

Note 2: This crime is only applicable to ATMs with motorized card readers, and with applications configured for ‘card before cash.’

NCR ATM SECURITY UPDATE

Mitigation:

1. This crime relies on the host application reversing the transaction based on status information from the card reader alone. Host applications MUST check the currency dispenser status prior to reversal of any transaction, any pre-positioned cash must be safely purged before authorization of a transaction reversal.
2. The S1 currency dispenser has anti-TRF settings known as EPS2 available which can be used to report potential fraudulent behavior. EPS2 can also change Transaction Codes such that it *may* be possible to prevent transaction reversal *without* host application changes.
3. The S2 currency dispenser can also be configured such that cash is not pre-positioned behind the shutter

NCR ATM SECURITY UPDATE

Alert Supplement
S2 General Security Guidance and Recommendations:

As well as protection against TRF, the S2 dispenser also supports a number of additional configuration options which can be used to deter and detect other forms of crime. NCR recommended settings are as follows:

Function	Purpose	Description
Programable pre-present "Pre-present enabled"	To prevent forms of Transaction Reversal Fraud e.g. by malicious card fault or shutter fault	Carriage can be programmed to remain at the rear of the dispenser, prior to shutter opening.
Programable Park "Idle Position"	To prevent access into the safe for the purpose of introducing explosive material (gas or solid)	The S2 note carriage can be programmed to lock in position blocking access through the dispenser transport into the safe
Programable Park "Idle Position"	To prevent possibility of reject bin fishing on front access ATMs	The S2 note carriage can be programmed to lock in position blocking access to the reject bin. Recommended for any front access ATM models.
Carriage Sweep "Carriage Sweep"	To detect the insertion of type 2 cash traps	The S2 carriage can be programmed to 'sweep' along the transport, prior to cash loading. This action will trigger a type 2 cash trap without exposing any currency

NCR ATM SECURITY UPDATE

Diagnostic Dispense Authentication "Dispense Enable Level"	To prevent misuse of diagnostic capabilities	All diagnostic commands that move currency can be disabled unless authorization is demonstrated
Tamper Sensors "Tamper Security Level" and "Tamper Recovery Procedure"	To detect anomalous behavior indicative of tampering, TRF, fishing	S2 sensors can be enabled to detect suspicious behavior, within the context of a transaction, and during idle time. Alert status can be sent to the application. S2 can be configured to automatically go out of service on detection of an alert.
Prepare for dispense Application Command	To offset any increase in transaction time	Programable Park can add 2 seconds to transaction time. This can be offset by an application modification to issue 'prepare for dispense'.

For more detail on these settings, please see APTRA XFS documentation.

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

Informational Webinars:

Join and engage Security and Fraud experts from NCR during a series of upcoming informational and interactive webinars. Click below to register for one of the upcoming NCR Secure webinar series:

Card Protection Trends and new Defense Solutions – July 10
How Fraud Protection fits into Security Strategy – July 18
Upgrading ATMs to Enhance Security – July 24

NCR ATM SECURITY UPDATE

NCR Security Summit

NCR will hold our 5th Annual Security and Fraud Summit on Oct 8, 2018 in London. This interactive executive session is focused on creating discussions on key issues and strategies for ATM Security and Fraud prevention.

Key topics will include:

- Discussion on the Windows 10 and its' impact ATM security, how NCR Security Solutions fit into the Windows 10 migration and what steps are needed to ensure protection during the migration
- The continuing growth of Fraud and how the ATM channel fits in to the situation and why Fraud protection must be part of your overall strategy
- New PCI Compliance requirements and deadlines are coming, learn from NCR and PCI experts as to what you need to do to remain compliant
- How NCR is looking to the future with new next generation ATM design, new security concepts and solutions
- And finish the evening at a dinner with your peers

But spaces at the NCR Security Summit are limited so please register today to secure your place at this event.

NCR ATM SECURITY UPDATE

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

For any further technical help on the information contained in this alert, please contact your usual NCR Support channel.