NCR ATM Security Update

DATE: July 22, 2020 **INCIDENT NO:** 2020-05 **REV:** #1

Black Box attacks on ATMs in Europe

NCR is aware of reports regarding recent Black Box attacks in Europe. These reports state that this is a new class of attack.

In this attack, it is claimed that the "Black Box" device, which connects directly to the Cash Dispensing Module, contains parts of the attacked ATM's software stack. The report states it is currently unknown how this is achieved but is under investigation.

While these attacks were not executed on NCR ATMs, we would like to take this opportunity to remind our customers that these types of attacks are attempted on all ATMs around the world. NCR advises our customers to follow our recommendations and solutions available to mitigate risks from these types of attacks.

We routinely update our **Best Practices for the Protection from Logical Attacks** which include our "15 Rules" which, when strictly followed, provide financial institutions with the best protection against this type of attack for their NCR ATMs.

Rules 7, 10 and 11 specifically and directly relate to protection against these Black Box attacks. The essential protections are:

- Set Dispenser security to the highest level
- Hard Disk Encryption
- The very latest Cash Module component (listed here)

Component	APTRA XFS Dispenser Release Package 01.00.00 Released om 13th February 2020
USBCurrencyDispenser	04.04.00
USBMediaDispenser	03.09.00
XFS CDM Service Provider	08.03.00
XFS MDM Service Provider	03.05.00
XFS Recycler Module Release Package PcGBRU & USB RM components	*APTRA XFS Recycler Module Release Package 01.00.00* released on 16th June 2020

As always however, NCR advise all 15 rules should be followed.

For any other questions or if you need further information on these topics please contact your NCR Representative.

Contacts

ATM Crime Reporting: Global.Security@ncr.com

Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com