NCR SECURITY UPDATE

DATE: May 5, 2016 **INCIDENT NO:** 2016-05 **REV:** #1

Expansion of Deep Insert Skimming Attacks

Summary

NCR has received additional reports of “Deep Insert Skimming Attacks”. To date there have been confirmed reports of attacks on all ATM manufacturers in Greece, Ireland, Italy, Switzerland, Sweden, Bulgaria, Turkey, United Kingdom and the USA. This suggests that ‘Deep Insert Skimming’ is becoming more viable for criminals as a tactic to avoid bezel mounted anti-skimming defenses.

Multiple variants of form factor of ‘Deep Insert Skimmers’ have now been observed in ATM with both Motorized and DIP card readers.

A Deep Insert Skimmer is different from a typical insert skimmer. These are a skimmer that is placed in various positions within the card reader transport, behind the shutter of a motorized card reader and completely hidden from the consumer at the front of the ATM.

These deep insert skimming devices are unlikely to be affected by most active anti-skimming jamming solutions. They are also unlikely to be detected by most fraudulent device detection solutions.

Guidance and Recommendations:

Neither NCR Skimming Protection Solution, nor other anti-skimming devices can prevent skimming with these Deep Insert Skimmers. This is due to the fact the skimmer sits well inside the card reader, away from the detectors or jammers of SPS.

NCR has developed a response to this attack, in the form of a modification to the card reader firmware. The firmware is designed to detect the insertion of the device, regardless of form factor, and send an alert.

NCR SECURITY UPDATE

The firmware will detect the insertion of the device, regardless of form factor, and send an alert. This firmware is currently in field trials, and once complete will be released as a standard function for NCR card readers. For installed ATMs, an APTRA XFS component upgrade will be made available. Please contact your NCR representative if you are interested in receiving the firmware, when it is globally available.

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: owen.wild@ncr.com