NCR SECURITY UPDATE

DATE: March 27, 2017 **INCIDENT NO:** 2017-02 **REV:** #1

Deep Insert Skimmer Attacks on DIP card readers

Summary

NCR has previously issued an alert on the emergence and expansion of Deep Insert Skimmers being used on motorized card readers. NCR has now received reports of Deep Insert Skimmer attacks targeting DIP card readers in the United States on both NCR and non-NCR ATMs.

A Deep Insert Skimmer is different from a typical insert skimmer. This is a skimmer that is placed inside the card reader by insertion through the card slot. Once in place, it is hidden from view to the consumer using the ATM. Use of Deep Insert Skimmers has emerged because they cannot be detected or jammed by anti-skimming equipment designed to prevent fraud through skimmers attached on the ATM fascia.

General Guidance and Recommendations for ATM endpoint security:

Since this new skimmer sits well inside the card reader and away from the detectors or jammers of the NCR Skimming Protection Solution (SPS) and other anti-skimming solutions used for detecting or jamming skimmers attached to the fascia, these are not effective for Deep Insert Skimmers.

Frequent and ongoing inspection of the ATM by trained personnel is highly recommended to attempt to identify if any skimmers have been inserted or attached to the ATM. Financial institutions can obtain more details on what to look for in a physical inspection of the ATM from NCR's **Fraud Inspection Guide**.

There are third party hardware products available which can be fitted inside the card reader and are designed to inhibit placement of the Deep Insert Skimmer. NCR does not endorse any particular product and is working on a hardware upgrade to address this type of fraud attack.

For motorized card readers, NCR will be releasing a software upgrade available for the APTRA XFS 6.05 platform software, scheduled for June.

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