NCR ATM Security Alert

DATE: January 20, 2023 **INCIDENT NO:** 2023-01 **REV:** 1

New “Deep Insert” Card Skimmer M.O. for DIP card readers

Guidance from NCR

NCR has been made aware of two separate successful skimming attacks against ATMs equipped with Tamper Resistant DIP Card Readers in USA.

The skimming technique is using a Deep Insert Skimmer in Tamper Resistant DIP Card Readers, but an additional attack step is performed that sabotages the internal workings of the Tamper Resistant DIP Card Reader. After this sabotage is performed, the skimmer can then operate inside the reader. Sabotaged readers show no signs of outward damage to the ATM user. Similarly, because the skimmer is placed inside the reader, these devices are almost impossible to spot by the typical ATM user.

Note: Deep Insert Skimmers cannot be detected or prevented by fascia skimming prevention solutions such as NCR SPS or third-party equivalents.

Customers are advised to be aware of possible signs of deep insert skimming. The most common indicator is impaired usability of the reader as the skimmer causes increased friction during card insertion and withdrawal; other indicators are card reading failures.

Skimming attacks also require the PIN, and the most common method of PIN capture is use of a covert camera hidden on the ATM. While Deep Insert Skimmers are very difficult to spot, PIN capture cameras are mounted on the outside of the ATM and can be found during inspection if staff are instructed to look for them. PIN cameras are typically hidden behind fake panels added to the ATM fascia. Common locations on NCR 80 Series ATMs are side panels in the PIN Pad recess; complete ATM side panels; or a false bar along the top of the fascia adjacent to the task lighting. Fake panels

that conceal a camera will have a small pin hole aperture to allow the camera to view the PIN pad. Any small holes observed in the vicinity of the PIN pad should be considered suspicious.

Card issuers can limit the impact of skimming by increasing the security checks on any magnetic stripe transaction authorization that originates from a chip card in an ATM. All North American ATMs are chip enabled, meaning that every chip card withdrawal should be processed as an EMV transaction. Any chip card transaction from an ATM which is processed using the magnetic stripe is a possible skimmed card. This information should be included in existing fraud detection profiling during the transaction authorization process.

Additional hardware upgrade countermeasures against this new M.O. are in development by NCR. A new model of DIP card reader with hardening against sabotage and internal skimmer detection sensors is scheduled for release at the end of Q1 2023. We will proactively notify customers when this new reader is available.

NCR continues to monitor and review reports of new attack vectors, and encourages customers to maintain a regular physical security review of ATMs in the field for any evidence of tampering.

Contacts

ATM Crime Reporting: Global.Security@ncr.com

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