NCR ATM Security Alert

DATE: September 15, 2022 **INCIDENT NO:** 2022-03 **REV:** 1

Media coverage on Deep Insert Skimming

Update and reminder of guidance and recommendations from NCR

On September 14, security journalist Brian Krebs reported on Deep Insert Skimming attacks in North America on his KrebsOnSecurity blog.

NCR alerted on these attacks in February 2022 in Alert 2022-02. This alert reiterates and provides updated guidance.

The skimming technique uses a new type of ultra-thin, Deep Insert Skimmer in motorized card readers. This skimmer can successfully operate inside the NCR Motorized Tamper Resistant Card Reader. The presence of the skimmer will significantly increase the probability of causing a card jam, but there is a reasonable likelihood that some cards can be successfully skimmed before a jam may occur, if at all.

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 a card jam; other indicators are card reading failures.

Skimming attacks also require the PIN, and the most common method of PIN capture is the use of a covert camera hidden on the ATM. 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 or complete ATM side panels. Fake panels that conceal a camera will have a small pinhole 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.

Additional hardware upgrade countermeasures for ultra-thin, Deep Insert Skimmers are in development by NCR. A mechanical inhibitor is now available for NCR customers to order, and an internal skimmer detection upgrade is scheduled for the early 2023.

Please contact your NCR or NCR partner representative for details.

Card issuers can limit the impact of skimming by increasing security checks on any magnetic stripe transaction authorizations that originate from chip cards 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 processed on an ATM using the magnetic stripe is vulnerable to skimming.

Contacts

ATM Crime Reporting: Global.Security@ncr.com

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