NCR ATM SECURITY UPDATE

DATE: June 30, 2017 **INCIDENT NO:** 2017-08 **REV:** #1

Eavesdropping Skimming Attacks on SelfServ™ ATMs in the USA

Summary

NCR has previously alerted you about the emergence and expansion of Eavesdropping Skimming attacks being used on Motorized Card readers on Personas model ATMs, predominantly in the UK. NCR now has reports of Eavesdropping Skimming attacks targeting motorized card readers on SelfServ ATMs in the United States.

Eavesdropping Skimming is a technique where the ATM fascia is penetrated to allow access to the card reader. A skimmer is then placed directly onto the card reader at a place where there is an electrical node that carries card data. Attacks on Personas ATMs targeted the card reader electronic control board, via a hole created behind the ATM card orientation window.

In these new attacks against SelfServ model ATMs, the method has been altered but the principle remains the same. These attacks represent a new variation as to how criminals are changing how they breach the ATM to gain access to the card reader

The ATM model targeted is the 6634, a Through-The-Wall (TTW) multifunction ATM. The attacker cuts a rectangular hole the in the side panel in between the ATM monitor and the card reader. This hole is then used to place an Eavesdropping Skimmer beneath the card reader, to connect directly to the card reader magnetic read head. The hole in the ATM is then disguised by fixing a color matched panel over the entire side panel of the ATM. See pictures below.

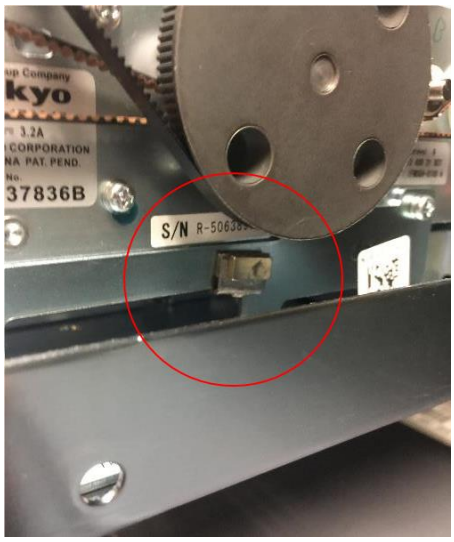
NCR ATM SECURITY UPDATE

PIN capture is typically achieved by placing a spy camera in the ATM light fitting above the key pad.

Hole in ATM Side Panel

Hole disguised with overlay

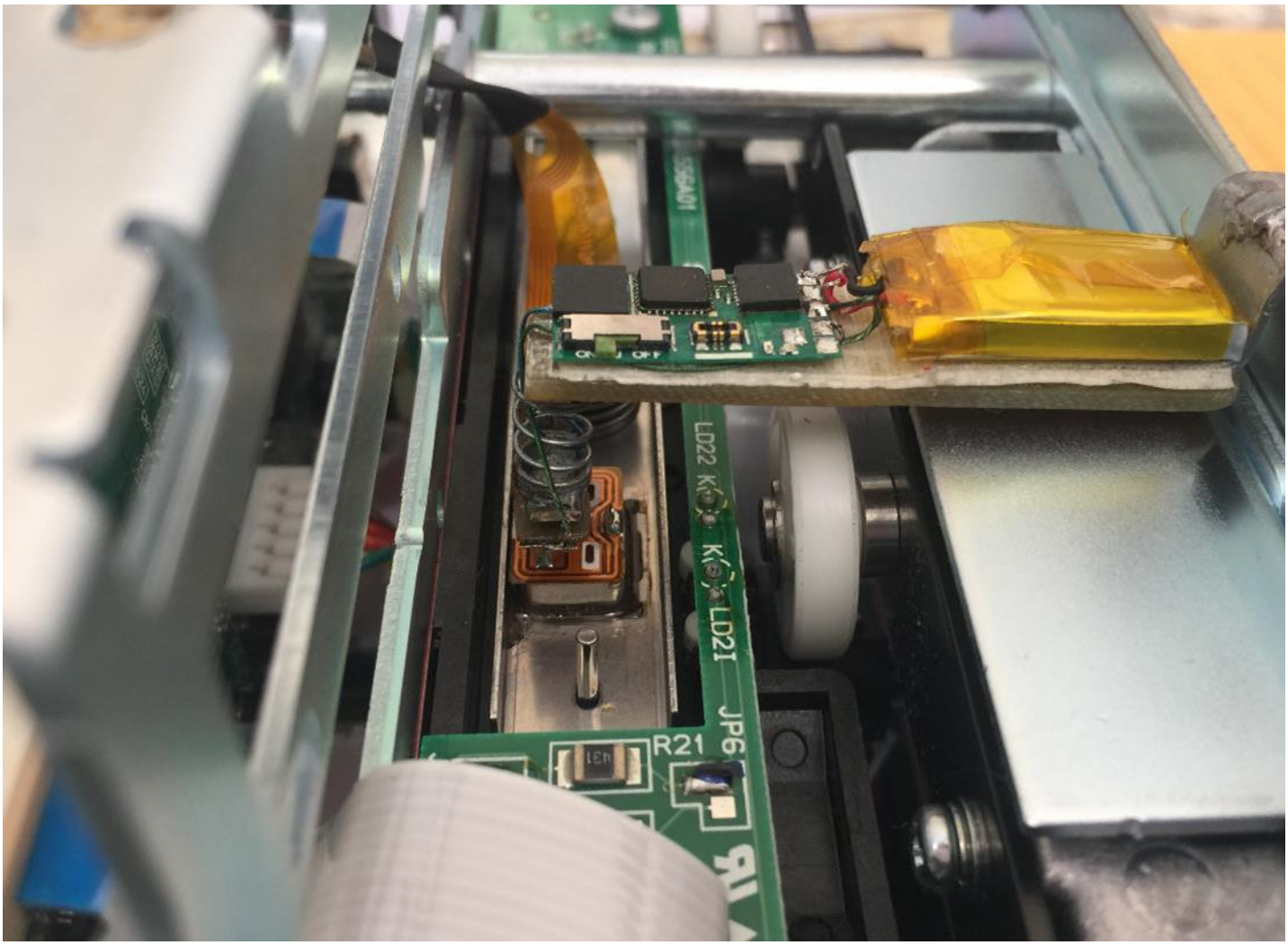
NCR ATM SECURITY UPDATE



Skimmer attached below card reader

Skimmer attached below card reader – viewed from below

NCR ATM SECURITY UPDATE



Close up view of skimmer attached below card reader

NCR ATM SECURITY UPDATE

General Guidance and Recommendations:

Frequent and ongoing inspection of the ATM is highly recommended to attempt to identify if any skimmers have been inserted or attached to the ATM. It is also critical that during these inspections extra attention be paid to attempting to identify if a camera has been installed to capture the PIN entry.

As noted, NCR Skimming Protection Solution, or other fascia fitted anti-skimming solutions, cannot detect or prevent Eavesdropping Skimming attacks. This is due to the fact the skimmer is fitted directly to the card reader, inside the ATM, away from the detectors or jammers of SPS located at the ATM fascia.

For motorized card readers, NCR has a solution in addition to SPS which will stop eavesdropping attacks in the form of the Anti-Eavesdropping Kit. This is available as both a factory fitted feature Product ID 66XX-F708, or as an upgrade kit Product ID 6634-K708-V003.

Contacts

ATM Crime Reporting : global.security@ncr.com
Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com
Media Inquiries or Questions: aaron.gould@ncr.com
Further information on this alert: owen.wild@ncr.com