NCR SECURITY UPDATE

DATE: September 8, 2015 **INCIDENT NO:** 2015-09 **REV:** #1

Card Shimming attacks on ATMs – clarification

Summary

NCR is aware that there has been broad press coverage of reported chip card attacks on Diebold ATMs in Mexico, and therefore offers the following commentary.

The form of attack known as Card Shimming is not a vulnerability with a chip card, nor with an ATM, and therefore it is not necessary to add protection mechanisms against this form of attack to the ATM.

The attack works by inserting a device into the ATM card reader that can intercept and record the data that flows between the chip card and the ATM reader. This data could then potentially be reused to then clone a magnetic card. However, the data that can be captured from a chip card cannot be reused to clone a magnetic strip, because chip data and mag strip data have different CVVs. (check values). This means that counterfeit cards can be immediately detected during transaction authorisation.

The only way for this attack to be successful is if an issuer neglects to check the CVV when authorising a transaction.

All issuers MUST make these basic checks to prevent this category of fraud.

NCR Skimming Protection Solution or any other anti-skimming solution is not intended nor designed to identify the attempted use of these Shimmer devices

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