# NCR SECURITY UPDATE

**DATE:** September 17, 2015 **INCIDENT NO:** 2015-11 **REV:** #1

## Bluetooth Skimming in Mexico

### Summary

NCR is aware of the recent blog reports of Bluetooth Skimming in Mexico, and we would offer the following commentary.

The attack MO is described as consisting of electronic devices that are installed inside the ATM that are capable of capturing card data and PIN data, and then using Bluetooth technology to transmit the data to the attacker. With the fraudulent devices on the inside of the ATM, there are no visible signs for the ATM user to know that skimming devices have been installed.

The critical factor to the success of this crime is the ability of the criminal to insert a PIN capturing device inside the ATM PIN pad. This is not possible on a modern NCR ATM equipped with a PCI compliant Encrypting PIN Pad. No NCR ATMs were involved in the Mexico fraud so we cannot comment on the specific technology that was compromised in those attacks. However, if an NCR EPP is disassembled in any way, any sensitive data within the device is immediately erased and the device is rendered permanently inoperable, as per PCI requirements.

### Guidance and Recommendations:

- **Deploy only PCI compliant EPPs running PCI compliant firmware.** NCR EPPs are designed such that it is infeasible for malware or internal taps to gain access to a plain text PIN.
- **Ensure that key loading procedures meet the security requirements of ISO 11568 and/or ANS X9.24.** Initial key loading is a sensitive function and must be treated accordingly. The EPP serial number must be verified as the expected serial number prior to loading any cryptographic keys. If an ATM service call necessitates a swap of the EPP, then the service call must be validated before cryptographic keys are loaded into the new device.
- **Use Remote Key Management as the method of key loading rather than manual key loading.** Remote Key Management means EPP cryptographic keys are transferred directly from the Host Security Module to the EPP in encrypted format, such that no individual will have access to the key.
- If manual key loading methods are employed, **key loading procedures that comply with ISO 11568 and/or ANS X9.24 must exist and be followed** to ensure the secrecy of the keys. Regular audits should be performed to ensure the procedures are followed. Audits should follow ANS TR39 or PCI PIN
- **Ensure that ATM cabinet is appropriately secured.** Prevent unauthorised personnel from accessing the interior of the ATM cabinet where they could tamper with the ATM controller or add ‘bugging’ equipment. This is particularly appropriate to free standing ATMs in unsupervised locations.

This and other frauds do not require the involvement of legitimate service technicians. NCR has a high degree of confidence in its service personnel in Mexico, who are aware of the risk of being approached to commit fraud and processes have been established to enable them to avoid such approaches, or respond to and report and approach if it occurs.

**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