NCR ATM SECURITY UPDATE

DATE: November 7, 2018 **INCIDENT NO:** 2018-11 **REV:** 1

Currency Theft from 6688 in North America

Summary

NCR has received multiple reports of thefts of cash from 6688 ATMs in North America. Most of the reports have come from Nevada and Texas, but customers should be aware that these thefts can spread, and that preventative actions must be taken on all 6688 models.

The method of the theft is by opening the ATM top box (sometimes called the “top hat”) and then by fishing notes from the currency dispenser reject bin, through the opening in the safe. The safe is not opened or breached. A key is required to open the ATM top box. All attacked ATMs were fitted with a common top box lock/key, and video evidence shows criminals are using a key to open the top box, indicating that they have obtained one or more of the common keys.

Recommendations to prevent theft

1. Any ATM located in an unattended, unprotected environment MUST NOT use common keys. All NCR ATMs are available with a choice of common, customer specific or ATM unique keys. For any ATMs in North America which are in unattended, unprotected environments, NCR strongly recommends immediate replacement of the common lock/key with a customer specific lock/key. NCR has kits available now which can be used for such replacement. This recommendation should be viewed as mandatory.
2. Any Front Access ATM with an S2 dispenser must be configured to park the carriage over the reject bin during idle operation. This function is known as Programmable Park, and

will prevent access to the reject bin when the ATM top box is open. NCR professional Services can assist with this configuration option.

3. Deploy defense in depth. Physical protection must always be complimented with appropriate monitoring and alarming; consider both silent and deterrent alarms upon unauthorized opening of the top box. Deterrent alarms may be implemented as sirens, lights, or smoke. Messaging can be added to the ATM screen to report that unauthorized access has been detected.
4. Keep dispenser software and firmware up to date. This ensures that any configuration recommendations can be applied and that the dispenser is protected against all currently known attacks. For the S2 dispenser, the minimum software/firmware is currently USBMediaDispenser 03.04.00, firmware 0x0118. This software can be applied using **APTRA XFS Dispenser Security Update 01.00.00.**

References:

1. **Security is Not an Option White Paper**: Cabinet Locks
2. **Security is Not an Option White Paper**: Dispenser Security Solution
2. **APTRA XFS Security Update Package 01.00.00** Release Notes

NCR ATM SECURITY UPDATE

Please contact your NCR Account Manager if you have any questions or need additional information.

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, please contact Owen Wild
Please refer any media inquiries or questions to Aaron Gould