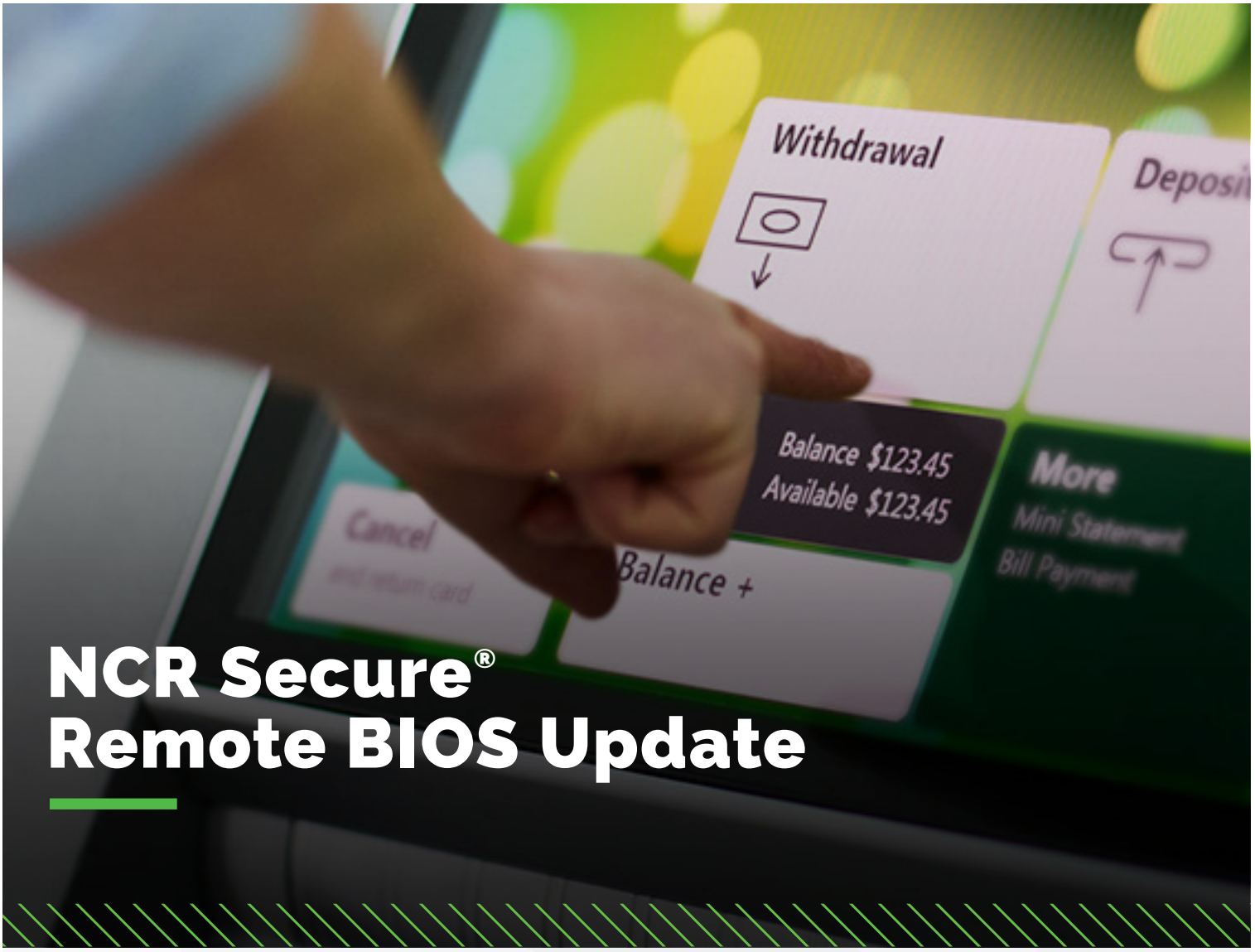

NCR Secure® Remote BIOS Update

Protection of the ATM BIOS is a critical component of comprehensive solution strategy to protect the ATM from Logical Attacks.

An unsecured BIOS allows criminals boot the ATM up from alternative bootable media. Once this is done, the ATMs hard disk operating system is no longer up and running (Offline) and this allows criminals to disable security measures that are in place on the ATM today (including any anti-virus solution). Once this is done, malware can be inserted on to the ATM's hard disk. This malware could be used to cash-out the ATM or to steal card data.

Intel's bug bounty program is meaning that BIOS Vulnerabilities are now being reported more frequently. For example, "Microarchitectural Data Sampling" (MDS) vulnerabilities. These side-channel attacks targeting Intel chips, allows hackers to effectively exploit design flaws in the processor architectures to extract sensitive data using malware so it is critical to keep BIOSes up to date with vulnerability fixes.

For more information, visit ncr.com, or email ncr.financial@ncr.com.

NCR

Key attributes of NCR Secure Remote BIOS Update

NCR Secure Remote BIOS Update

Flashes the BIOS to:

- Only allow boot from primary hard drive (Disallow boot from CD/USB).
- Add a default BIOS password to all the ATMs in a Financial Institution's network.
- Set up unique UUIDs per ATM.
- Update the BIOS to resolve any known vulnerabilities.
- Enable no-touch password implementation and maintenance.

Provides the ability to:

- Change the default password to a new secure password of your choice. No flash. No ATM reboot needed.
- Update password anytime (daily/weekly/monthly etc.).
- Update the boot order to USB/CD/DVD/PXE to allow for access where necessary.
- Set the boot order back to Hard drive only to lock the BIOS back down/ No flash. No ATM reboot needed.
- Check which device is currently set as the primary bootable device.
- Check there is a password set (where there is not one mandated to be set).
- Check the BIOS version without performing flash operation.
- Update the BIOS to resolve any known vulnerabilities.
- Enable no-touch password implementation and maintenance.

For most NCR Windows 10 compatible cores:

- Reset BIOS password (forces you to enter a new password) for forgotten passwords.
- Update BBS password.
- Flash over same version (need to know password).
- Ability to Set/query PXE Boot remotely.
- Ability to keep current LAN port or enable both LAN ports.
- Ability to set AMT remotely.
- Ability to keep the old password during the flash process.
- Ability to boot to alternative media for a specified number of reboots or for a specific duration of time.

NOTE: For Windows 10 compatible cores (not Falcon), the ATM Hard Disk is whitelisted in the BIOS, so trying to boot from another hard disk or replacing a hard disk is not possible). This is a feature of the newer BIOS rather than RBU.

Why NCR?

NCR Corporation (NYSE: NCR) is a leading software and services-led enterprise provider in the financial, retail, hospitality, small business and telecom and technology industries. We run key aspects of our clients' business, so they can focus on what they do best.

NCR is headquartered in Atlanta, GA with 34,000 employees and solutions in 141 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

171942-BANKING_ENDPOINTSECURITY-0520 ncr.com