Cyber and Physical Security Threats

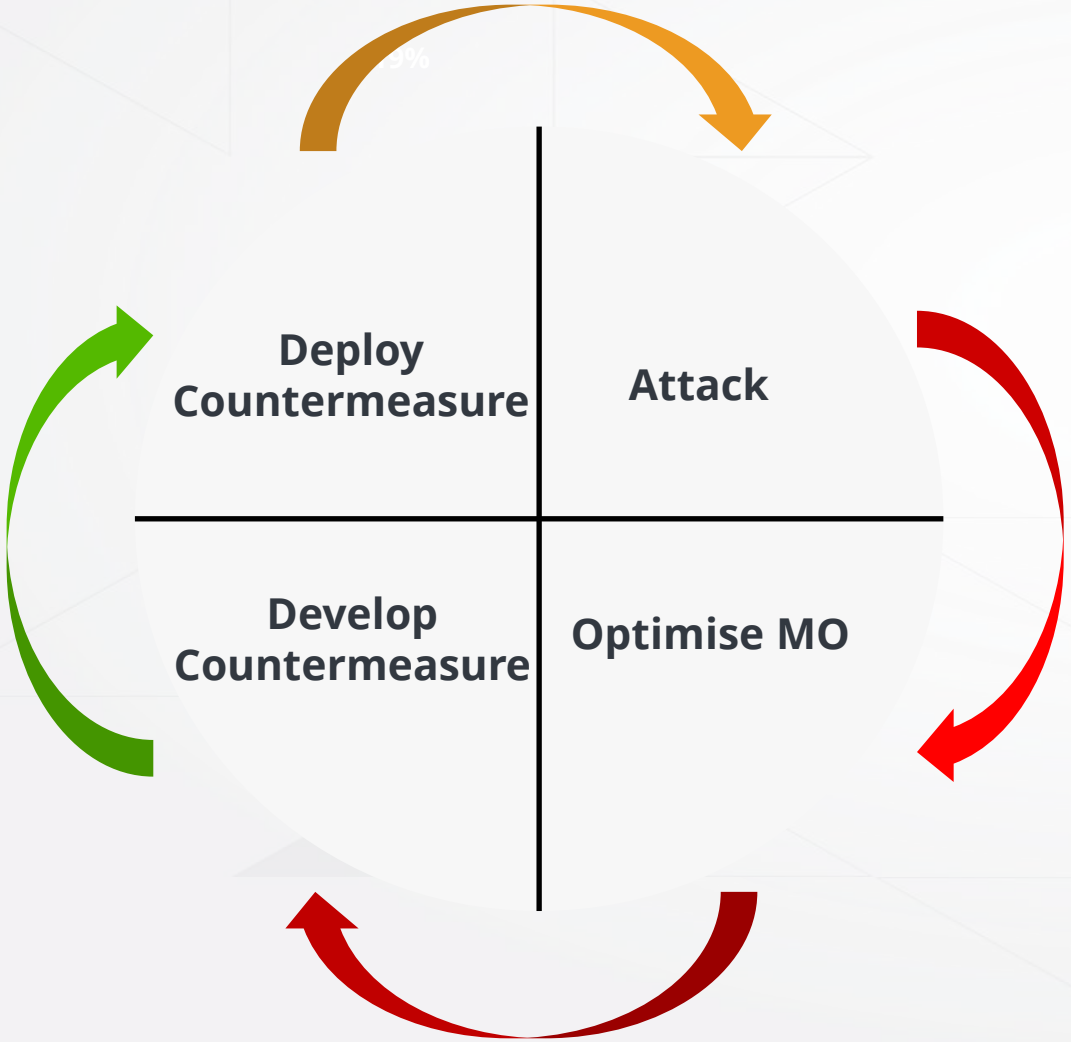
Paul Cowley – VP Technical Support and Logistics, DBE

Why Should You Trust Me?

- 20 years in the ATM service delivery industry
  - Design and implement security processes and procedures
  - Protect against and respond to ATM attacks
  - Develop partnerships within industry and law enforcement

- Active participant in ATMIA (ATM Industry Association)
  - Security-related Committees
  - Security Conferences
  - Annual Conferences

ATM Crime - Modus Operandi Evolution Cycle



4 phases of 'Attack / Countermeasure' cycle

- **1st and 2nd** phases – an attack vector may see many iterations until MO is optimised by the criminals – nearly limitless testing and no budget resource pressures as seen in industry
- **3rd Phase** – OEMs, Partners, and FIs developing protection
- **4th Phase** – deployment of countermeasure

- **Cycle begins again with a new attack vector**

ATM Attack Categories

Logical / Data Attacks

- Skimming
- Eavesdropping
- Man-in-the-Middle/Host Spoofing
- Black Box
- Malware
- Data Loss/Compromise

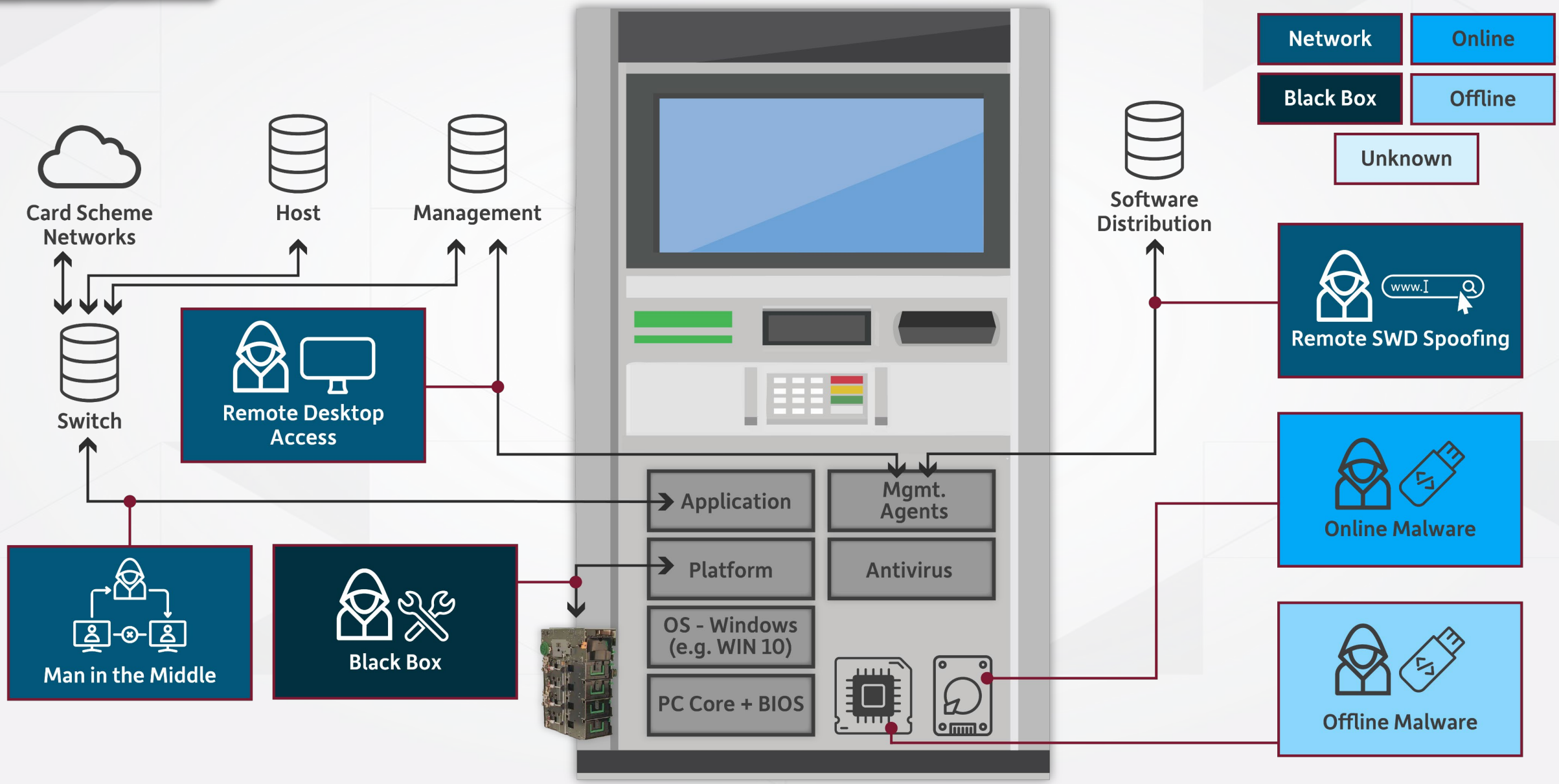
Physical Attacks

- Transaction Reversal Fraud
- Cash Trapping
- In-situ Tools
- Rescue Tools - ‘Jaws of Life’
- Ram-Raid/Pull-Out/Hook and Chain
- Explosives

“Jackpotting”

- Online Malware
- Offline Malware
- Man-in-the-Middle
- Black Box

Logical Attacks



Offline Malware Attacks

Latest version observed in Mexico in early 2023

- ATM vendor-agnostic, referred to as FiXS
- Currently a known, active exploit against Diebold and Hyosung machines

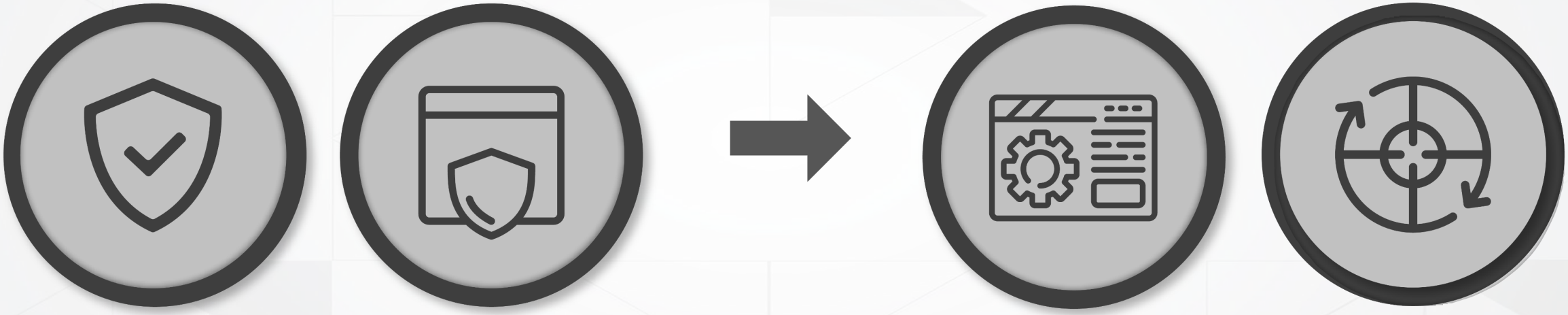
New iteration of previous malware, but works with the same MO as Ploutus (first observed in 2013)

- Typically introduced by physical access (e.g. USB stick or remove/replace HDD)
- Evolved to make the malware harder to reverse engineer and defeat

Logical Attacks – Malware

- Countermeasures include:
  - Lock down BIOS and all machine configuration menus
  - Harden the Operating System (OS)
  - Ensure monthly OS security updates are being installed
  - Ensure platform software is patched and updated regularly
  - Upgrade software that has exceeded OEM support lifecycle
  - Replace hardware that has exceeded OEM support lifecycle
  - Control physical access
    - Monitored alarms on ATM ‘top box’ area
      - Physical barriers
      - Custom keying solutions
  - Deploy hard disk encryption and anti-malware solutions

Logical Attacks – Creating an Offensive Posture



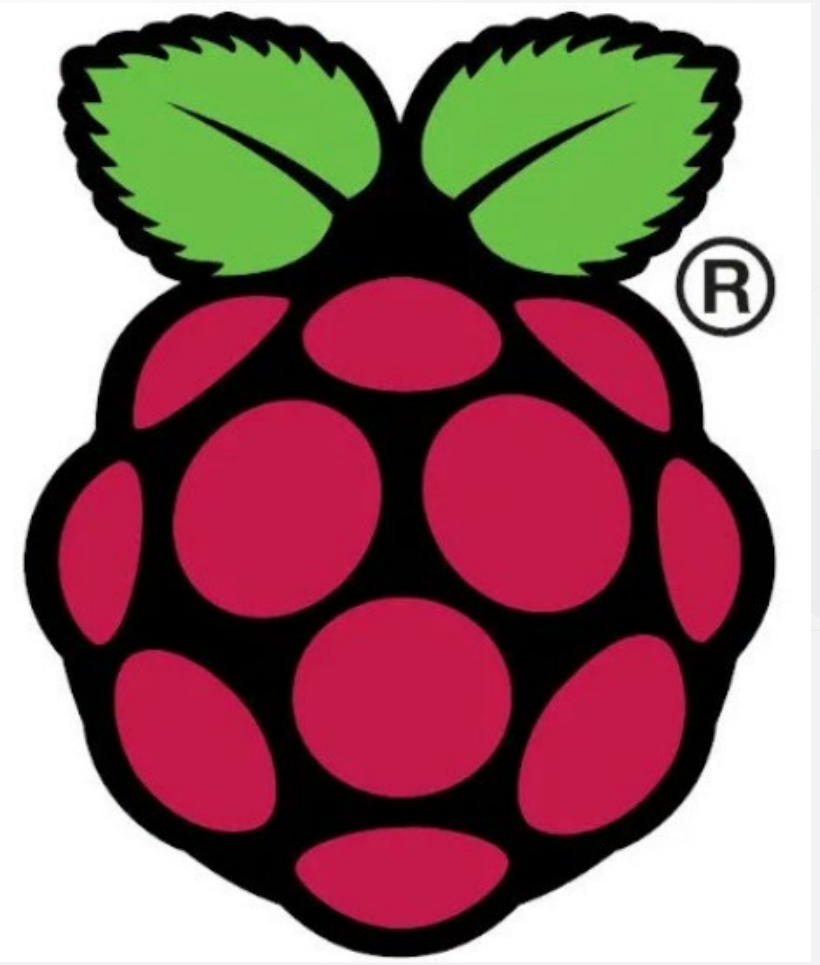
Host Spoofing / ‘Man-in-the-Middle’ (MITM)

Increasing threat since Q3 2023

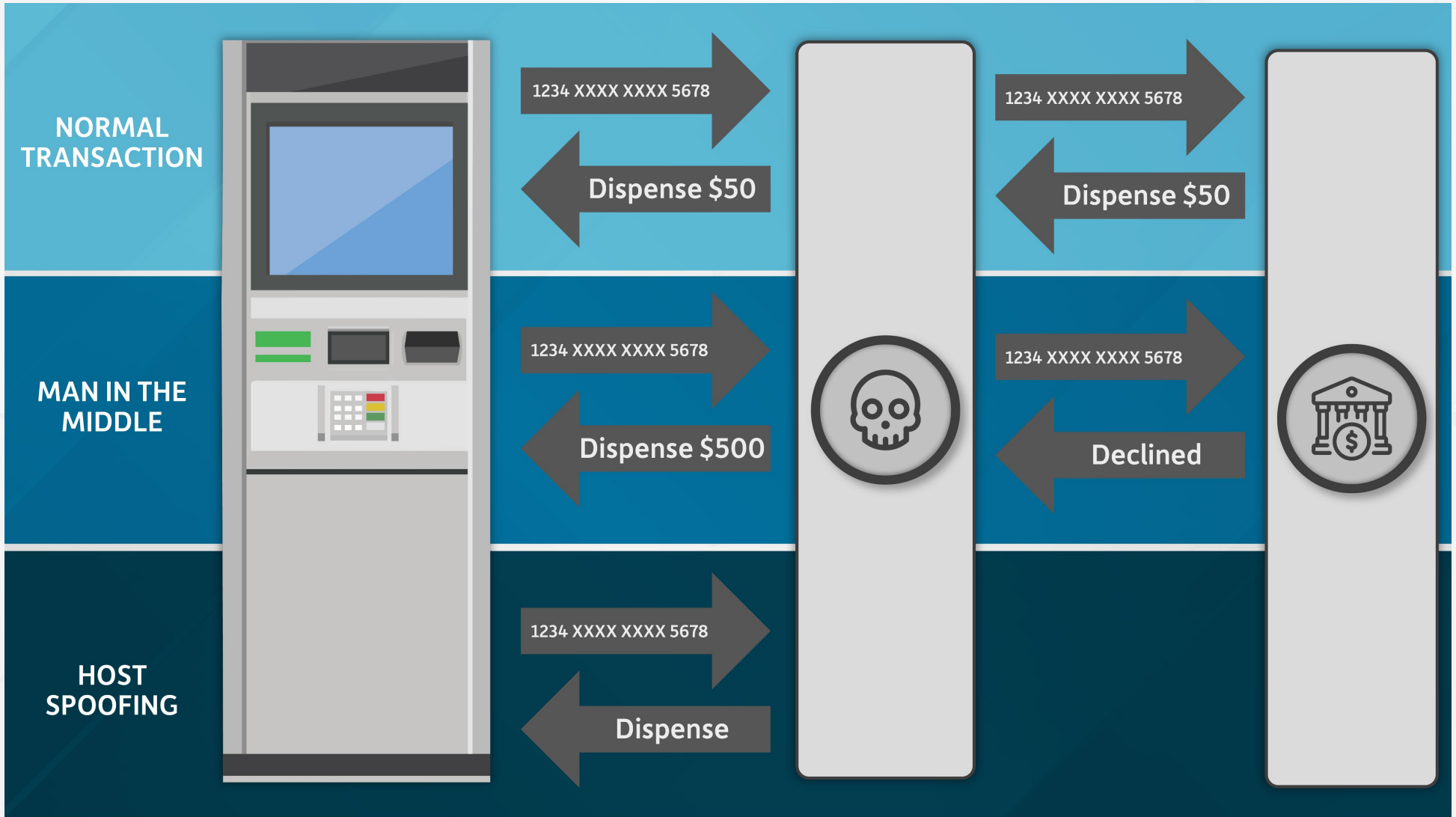
- Currently targeting machines using NDC Host messaging
- First attacks observed in Texas mid-year 2023
- Known attacks confirmed broadly across the US
- Results in a complete ‘cash-out’ of the ATM over 60-90 minute span

Access to the ATM ‘top box’ is obtained and the network cable is removed. A RaspberryPi SBC with custom software is connected in place of the network cable

- Frequently targeting smaller FIs
- Belief is that the bad actors assume a less-robust investment in security countermeasures by smaller FIs



Host Spoofing / ‘Man-in-the-Middle’ (MITM)



Logical Attacks – Host Spoofing/'MITM'

- Countermeasures include:
  - Enable end-to-end encryption on Host communications using TLS1.2
  - Protect network configuration menus with passwords
  - Control physical access
    - Monitored alarms on ATM 'top box' area
      - Physical barriers
      - Custom keying solutions
  - Ensure monthly OS security updates are being installed
  - Ensure platform software is patched and updated regularly
  - Utilize PCI TR-31 and TR-34 protocols for encryption keys
  - Deploy hard disk encryption and anti-malware solutions

Logical Attacks – Black Box

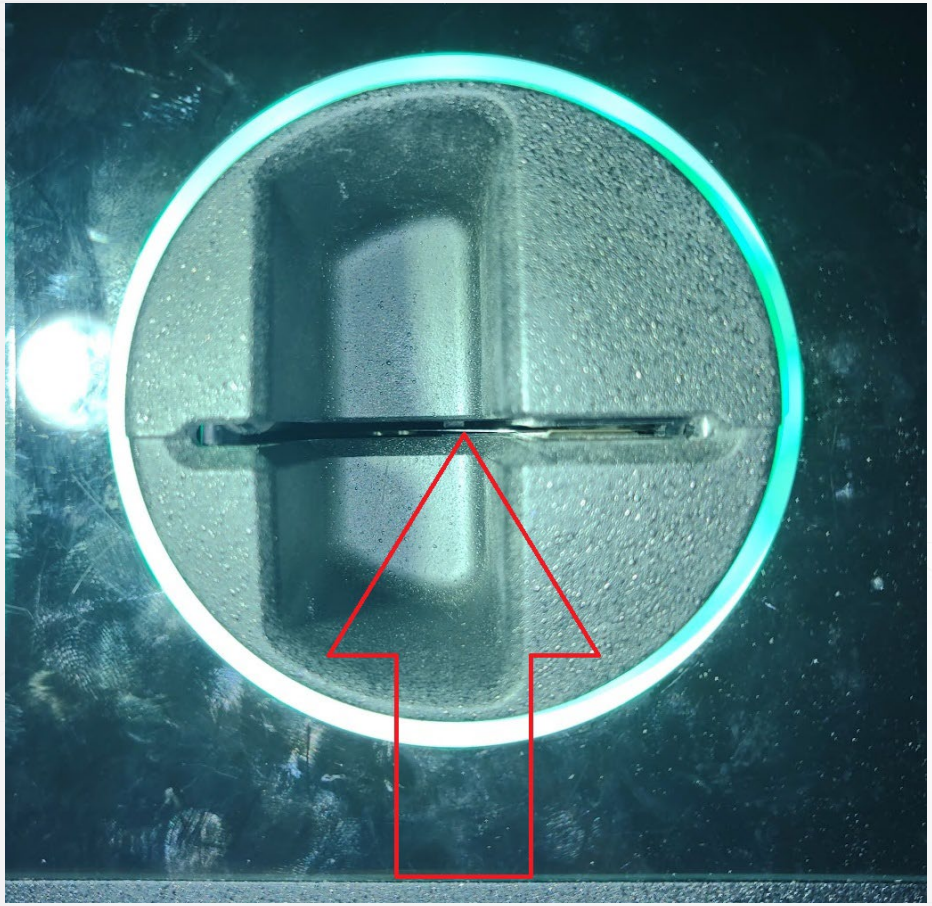
- Standalone electronic device that sends dispense commands directly to the cash dispenser

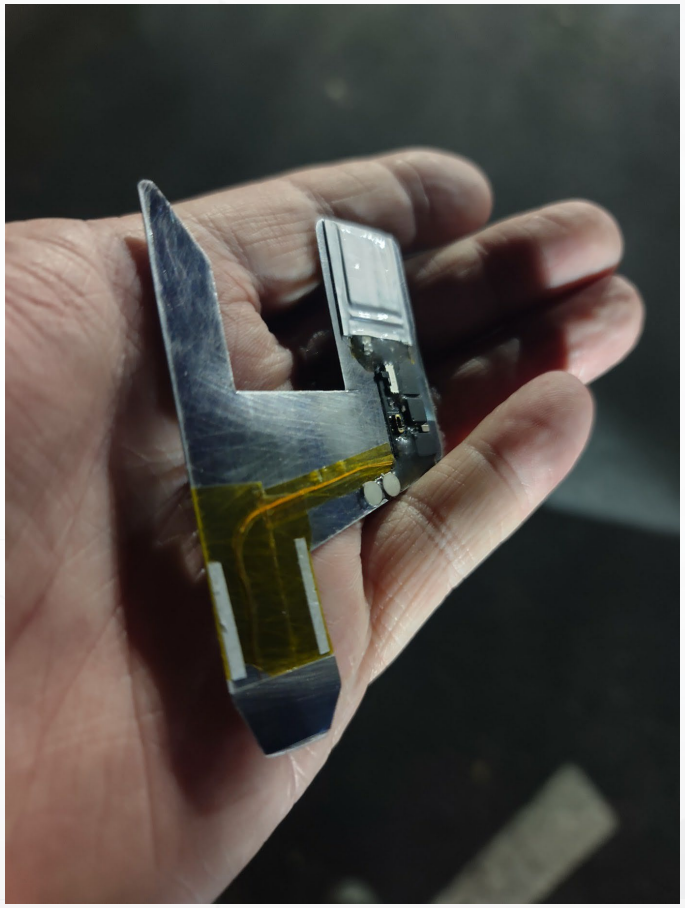
- Countermeasures include:
  - Replace ATMs that have exceeded OEM support lifecycle
  - Ensure platform software is current and patched/updated regularly
  - Ensure OEM cash dispenser authentication recommendations are fully implemented
  - Control physical access
    - Monitored alarms on ATM ‘top box’ area
      - Physical barriers
      - Custom keying solutions

Operating System Support Lifecycle

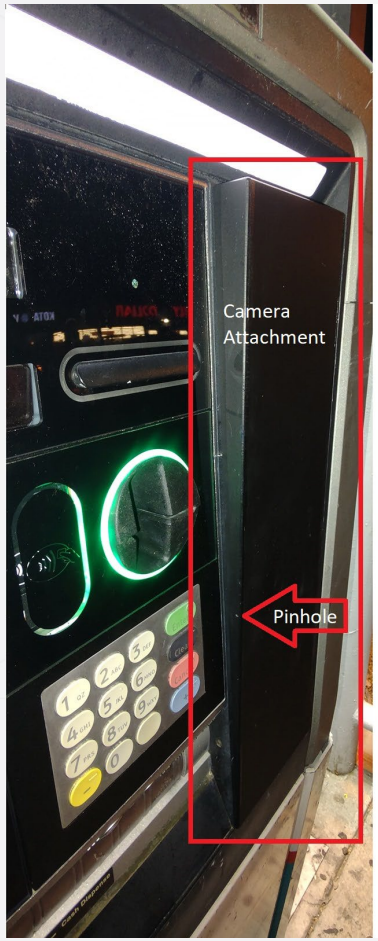
- Largest ATM vendors deploy IoT Enterprise LTSC versions of Windows
  - Long-Term Support Channel releases (i.e. Windows 10 IoT Enterprise LTSC v1607, v1809 or v21H2)
  - Microsoft commitment to support for 10 years from release date
  - New version typically released every 2-3 years
    - Unlike 'consumer' Windows releases, updates require purchase of a new Microsoft license
    - New release versions may not support older PC core hardware
- NCR Activate Enterprise (as currently deployed by DBE) => W10 LTSC v1809 license with support through January 2029
- Windows Embedded/CE 8.0 "extended" support ended October 2023
  - Windows Embedded Compact 7.0 (2021)
  - Windows Embedded CE 6.0 (2018)
  - Windows CE 5.x (2014)

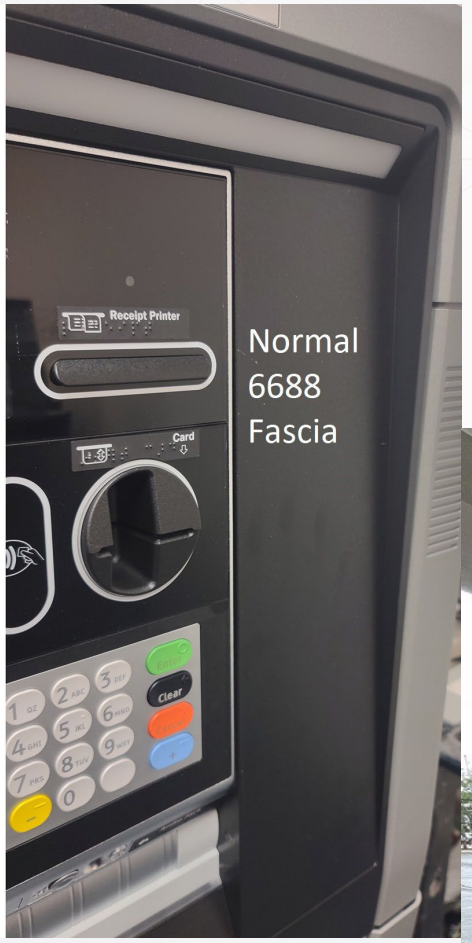
Ultra-thin Deep-insert Skimming Attacks

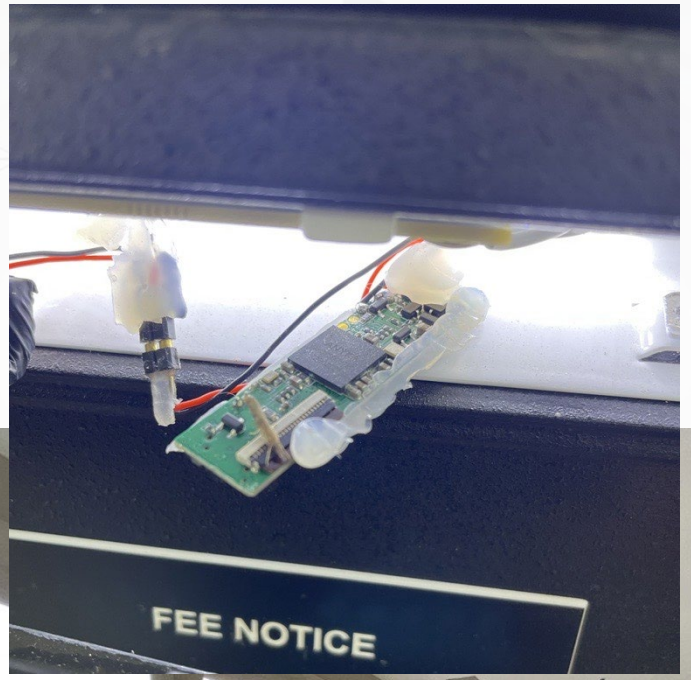




Ultra-thin Deep-insert Skimming Attacks







Tools to Stop the Skimming “Arms Race”

Card skimming remains a problem because it is too easy for a criminal to capture and reuse the static Track 2 data found on magnetic stripe cards

- Contactless EMV / NFC
  - Educate users about increased security offered by contactless transactions
  - Contactless EMV uses unique cryptograms in each transaction which cannot be reused if captured
  - The elimination of card insertion eliminates the opportunity for fascia AND deep-insert skimming
  - Disable EMV fallback transactions
- Tamper Detecting Card Reader (TDCR)
  - Devices as thin as 0.5mm so passive space restriction is no longer an effective countermeasure
  - TDCR is available as an in-place upgrade to all currently-supported NCR ATMs
  - Now a standard feature on all DBE-supplied ATMs manufactured after 8/1/2023
  - Software integration for TDCR detection capability requires Activate Enterprise 3.8 software
- Skimming Protection Solution (SPS)
  - Still the best-available option for preventing ‘overlay’ skimming

Physical Attacks

Physical Attacks

- Transaction Reversal Fraud
- Cash Trapping
- In-situ Tools
- Rescue Tools - ‘Jaws of Life’
- Ram-Raid/Pull-Out/Hook and Chain
- Explosives

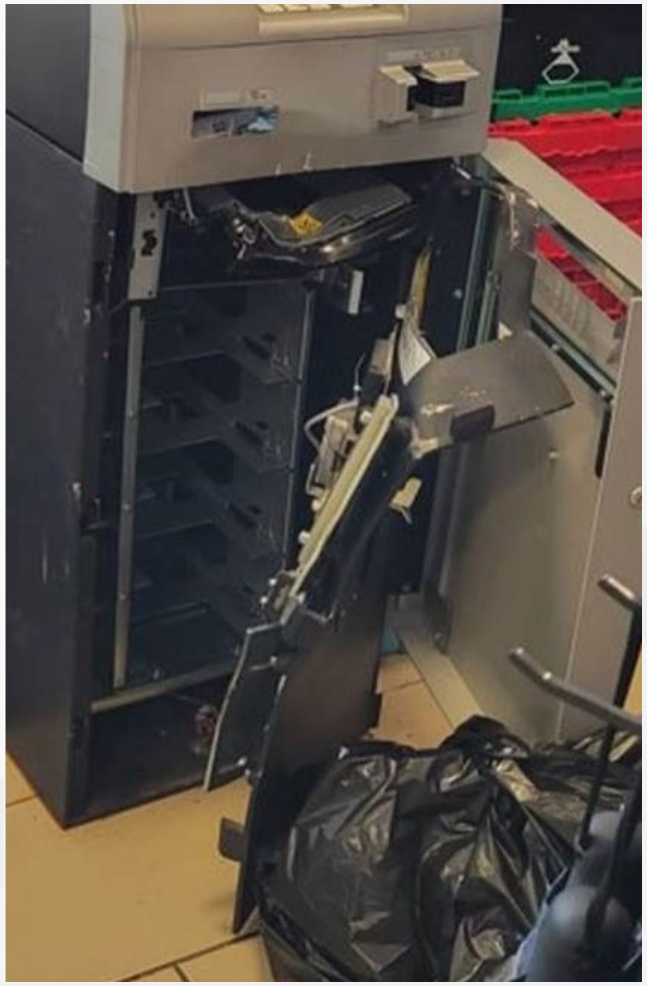
Transaction Reversal Fraud and Cash Trapping

- Protections include:
  - Ensure ATM platform software is current and patched regularly
  - Physical add-on countermeasures

‘Jaws of Life’ Attacks

- Emerging attack being reported across the US
  - Begins with theft of hydraulically-powered public safety rescue equipment
  - VERY effective attack on UL Level 1 and Business-Hours rated security enclosures
  - Given enough time, even CEN-I rated vaults have been compromised

‘Jaws of Life’ Attacks



‘Hook and Chain’ Attacks

- Brute-force attack STILL being widely employed across the US
  - Begins with the theft of a vehicle (typically medium-duty truck)
  - Typically targets older-generation island ATM/ITMs with sufficient site access
  - Utilizes heavy chain or cable to forcibly remove the safe door
  - Successful attacks against ALL makes, including Hyosung, NCR, and Diebold Nixdorf machines
- Average loss per incident is estimated at approximately $120k
  - Equipment, Safe Contents, and Site Damage

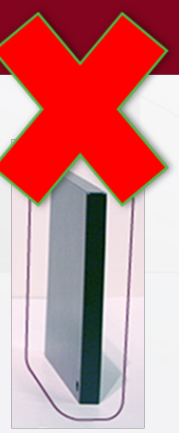
‘Hook and Chain’ Attacks

Physical Attack Countermeasures

- Deploy new machines with higher security ratings

UL291 Level 1 (24 hour)

- Tested for door attack only
- 15mins (common mechanical tools)
- Lower grades uses "hand tools" only for attack testing
- Construction requirements defined in spec must be met
- High tensile steel walls
- Discontinued in favor of CEN safes



CEN L

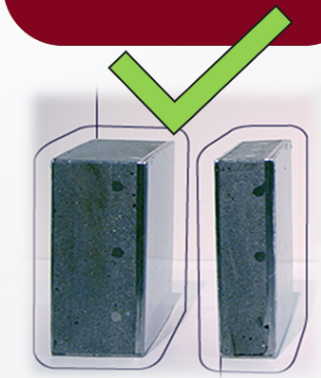
- Steel door skin and steel outer shell filled with concrete composite mix
- Superior safe door with more resistance to thermal attacks
- Discontinued in favor of CEN I safes

CEN I

- Body is the same strength as the door (CEN L standard allows a weaker body)
- Offers 66% more resistance to full access attacks and 50% more resistance in attacks to remove cassettes on the CEN I body
- Steel door skin and steel outer shell filled with concrete composite mix
- Body 40mm thick
- Relockers used in case of breach of lock to secure door
- One lock required and tested as part of the EN 1143-1:2019 standard
- Not designed to withstand explosive attacks
- Weight 478 kg
- Discontinued on island drive up units in favor of CEN III GAS-EX

CEN III GAS-EX

- Sheet steel outer and inner skin, with concrete in between.
- Additional grid-like reinforcement welded within inner body
- Concrete composite includes hardened particles
- Additional top and bottom bolts
- Additional hooking bolts to contain explosions but allow energy to expel
- Additional reinforcement of corners
- Offers 2 ½ more resistance to cutting attacks than CEN I
- Body 40mm thick
- Weight – 603 kg
- Same footprint as CEN I



Other Physical Security Considerations

- Adopt a layered and preventative approach to addressing physical attacks – BEFORE they happen
- Evaluate ATM locations and risk environments regularly
- Consider security impacts of site design whenever possible
- Install and maintain remotely-monitored alarms on both the ATM top box AND vault/security enclosure
  - Additional alarm zone on kiosk or building if ATM is through-the-wall
- Leverage intelligent video surveillance solutions
- Utilize high-security electronic locks for access to ATM safe
- Consider deploying IBNS (Intelligent Banknote Neutralization System - 'note staining') functionality

PCI Compliance Mandates - 2025

- TR-31 – Key Block support
- TR-34 – SHA-256 support for Remote Key Loading (RKL)

- Enforcement has been deferred to network host processors
- Requirements vary by network host processor
  - Certain host processors may have more stringent requirements
- Contact your host processor for more information on requirements and specific deadlines for compliance

Data Business Equipment, Inc.

Q & A