

# ATM & POS TERMINAL SECURITY.



ATMs and POS terminals are the physical hardware where card-present fraud actually happens — skimmers on the card slot, cameras over the keypad, malware on the machine itself. **EMV chip cryptography stops cloning, but it doesn't stop a device attacker from capturing data or an ATM from being commanded to dispense cash directly.**

- SKIMMING & SHIMMING
- ATM JACKPOTTING
- TAMPER-EVIDENT HARDWARE
- POINT-OF-CAPTURE ENCRYPTION

## 01 THE MECHANISM

### Skimming Captures the Stripe, Not the Chip

A physical device attached to or inserted into the card slot reads magnetic stripe data as a card passes through, **typically paired with a hidden camera or fake keypad overlay** to capture the PIN separately.

### Jackpotting Targets the Computer, Not the Account

Malware installed on an ATM's internal computer commands the cash dispenser directly, **bypassing the card and account system entirely** to dispense cash on demand.

### Tamper-Responsive Hardware Fights Back

PCI PTS-certified terminals are built to detect physical tampering and **automatically erase their own cryptographic keys** the moment intrusion is detected.

## 02 THE FLOW

### The Hardened, Inspected Terminal

CONTAINED

1

Staff conduct regular, unpredictable physical inspections comparing each terminal to its known appearance, **catching an added skimmer before it captures a single card.**

2

The terminal encrypts card data at the point of capture, inside its own tamper-resistant hardware, so a **compromised POS system never holds cleartext card data.**

3

The ATM's software is locked to an explicit whitelist and its ports physically secured, so a **USB-delivered jackpotting attempt has nothing to execute.**

### The Unwatched, Unhardened Terminal

EXPOSED

1

A skimmer and hidden camera go unnoticed for days on an unmonitored terminal, **quietly capturing card and PIN data** from every customer who uses it.

2

The POS system processes card data in cleartext in memory before encrypting it for transmission, leaving a **window RAM-scraping malware is built to exploit.**

3

An exposed USB port and an unpatched, unrestricted operating system give jackpotting malware **everything it needs to command the cash dispenser** directly.

## 03 CORE PILLARS & COVERAGE

| PILLAR                                    | WHAT IT COVERS                                                                                                                                      |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamper-Evident Hardware                   | PCI PTS-certified terminals designed to detect physical intrusion and automatically erase cryptographic keys the moment tampering is detected.      |
| Point-to-Point Encryption                 | Encrypting card data at the point of capture inside the terminal itself, so cleartext data is never available in the connected POS system's memory. |
| Physical Inspection & Monitoring          | Regular, unpredictable checks comparing terminals against their known appearance to catch skimmers, shims, or keypad overlays.                      |
| Software Integrity & Network Segmentation | Application whitelisting, port lockdown, and isolating ATM/POS networks from the general corporate network.                                         |

## 04 DETECTION APPROACHES COMPARED

| APPROACH                                                                            | SUFFICIENT ALONE? | WHAT IT MISSES                                                                                                                                                           |
|-------------------------------------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EMV Chip Alone, No Terminal Hardening                                               | No                | Chip cryptography resists cloning, but skimming and shimming devices still capture data usable for magstripe-fallback fraud, and jackpotting bypasses the card entirely. |
| Encrypting Transmission Without Point-of-Capture Encryption                         | No                | If card data sits in cleartext in POS system memory before encryption, RAM-scraping malware can still capture it.                                                        |
| Occasional, Predictable Inspection Schedules                                        | No                | A predictable inspection routine gives an attacker a known window to install and retrieve a skimming device between checks.                                              |
| Unrestricted ATM Software and Open Ports                                            | No                | An ATM with no software whitelisting and an accessible USB port gives jackpotting malware a straightforward path to the dispenser.                                       |
| Tamper-Responsive Hardware + P2PE + Unpredictable Inspection + Locked-Down Software | Yes               | Closes the physical, memory, and software layers an attacker actually has to work through.                                                                               |

ATM & POS TERMINAL SECURITY.

INSPECT · ENCRYPT · RESTRICT

05 PROGRAM OPERATIONS

EMV chip cryptography makes cloning a chip computationally infeasible with current techniques, which is exactly why the 2015 US liability shift pushed merchants toward chip-capable terminals.

Skimming and shimmming are physical, add-on attacks — the front-line defense is simple physical inspection, not a software control, since the device has to actually be attached to the terminal.

Jackpotting bypasses the card and account system entirely by attacking the ATM as a computer, which is why software whitelisting and port lockdown matter as much as transaction-layer protections.

ATM and POS networks share real structural similarities with OT environments — purpose-built, hard-to-patch, physically distributed endpoints that shouldn't sit flatly on the general network.

06 CONTROL MAPPING

PCI PTS

PIN Transaction Security — the PCI SSC standard specifically for payment terminal and device hardware security, distinct from PCI DSS's broader merchant scope.

PCI P2PE STANDARD

Validated point-to-point encryption solutions, certifying that card data is encrypted at the point of capture inside tamper-resistant hardware.

EMV LIABILITY SHIFT (2015)

The US policy change that shifted counterfeit-card fraud liability toward merchants who hadn't adopted chip-capable terminals.

FBI/SECRET SERVICE ADVISORIES

Law enforcement alerts documenting real-world ATM jackpotting campaigns and the malware families behind them.

07 WHAT THIS DOES NOT SOLVE

Card-Not-Present Fraud

Terminal hardening protects the physical, card-present transaction; it does **nothing for online or phone transactions** where no physical terminal is involved.

Insider Collusion at Installation

Tamper-evident hardware and inspections assume an outside attacker; an **employee with authorized access** can bypass some physical checks entirely.

Upstream Network or Processor Compromise

A hardened terminal doesn't protect against a compromise **further up the chain**, at the network switch, processor, or acquiring bank's own systems.

Social Engineering at the Terminal

Physical and software hardening doesn't stop a customer from being **talked into a fraudulent transaction** or handing over a card and PIN directly.

08 MYTHS VS. REALITY

|                                                                                                  |                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>MYTH</div> <div>"EMV chip cards can't be skimmed."</div>                                    | <div>REALITY</div> <div>Skimming and shimmming devices can still capture data during a chip transaction; the chip resists cloning, but <b>captured data can sometimes still enable magstripe-fallback fraud</b>.</div> |
| <div>MYTH</div> <div>"Jackpotting requires hacking into the bank's network."</div>               | <div>REALITY</div> <div>Most jackpotting attacks install malware through <b>physical access to the ATM's own computer</b>, often via an exposed USB port, not a network breach.</div>                                  |
| <div>MYTH</div> <div>"If the terminal looks normal, it hasn't been tampered with."</div>         | <div>REALITY</div> <div>Modern skimmers, especially deep-insert models, can sit <b>entirely inside the card slot</b> and be effectively invisible without a detailed inspection.</div>                                 |
| <div>MYTH</div> <div>"Encrypting the connection to the processor is enough."</div>               | <div>REALITY</div> <div>Without point-of-capture encryption, card data can sit in cleartext in the POS system's own memory, <b>exactly where RAM-scraping malware looks</b>.</div>                                     |
| <div>MYTH</div> <div>"ATM/POS security is the same problem as general PCI DSS compliance."</div> | <div>REALITY</div> <div>PCI PTS specifically governs the <b>terminal hardware itself</b>, a distinct standard from PCI DSS's broader merchant-environment scope.</div>                                                 |

09 SPEAK THE PROGRAM — KEY TERMS

SKIMMING

A physical device attached to or inserted into a card reader that **captures magnetic stripe data** as a card passes through.

SHIMMING

A thinner device inserted into the card slot to capture data during an EMV chip transaction, **distinct from cloning the chip itself**.

JACKPOTTING

Malware that commands an ATM's cash dispenser to dispense cash directly, **bypassing the card and account system entirely**.

RAM SCRAPING

Malware that captures payment card data from a system's memory **during the brief window before encryption** is applied.

PCI PTS

The PCI SSC standard for payment terminal hardware security, covering **tamper resistance and cryptographic key protection**.

POINT-TO-POINT ENCRYPTION (P2PE)

Encrypting card data at the point of capture inside tamper-resistant hardware, **before it ever reaches the connected POS system**.