CORNELIUS SYSTEMS

CRACKING THE CODE: DEFENDING AGAINST ATM AND ITM EXPLOITS IN A MODERN THREAT LANDSCAPE

Whitepaper by Marvin Bowers and Tim Boehne

Evolving Fraud Techniques

ATM Security

Layered Defense Strategy

877-545-5558 www.mycornelius.com

Cracking the Code: Defending Against ATM and ITM Exploits in a Modern Threat Landscape

---

Chapter 1: The Modern Threat Landscape

The modern ATM is no longer an isolated machine. It's a connected endpoint—tied into networks, software platforms, and, increasingly, the customer experience. While those connections have enhanced functionality and efficiency, they've also broadened the attack surface in ways that legacy strategies were never designed to handle.

Three primary threat categories are dominating the risk conversation in 2025:

- **Jackpotting**, where attackers use malware or external devices to manipulate the dispenser logic and withdraw cash without authorization.
- **Skimming and Shimming**, where fraudsters steal card and PIN data through hidden devices that are now smaller, smarter, and harder to detect.
- **ITM Loan Exploitation**, where bad actors use interactive teller systems to access unsecured credit products by leveraging synthetic identities and weak verification protocols.

These methods aren't new, but their effectiveness is increasing as attackers refine their techniques and capitalize on operational blind spots. In recent incidents tracked by the U.S. Secret Service and FS-ISAC, coordinated fraud rings have moved across multiple states targeting both retail and financial institution machines. Notably, the convergence of remote access software, outdated security practices, and growing machine complexity has introduced new layers of exposure.

For financial institutions, the question isn't whether they'll be targeted, but whether their current policies and partners can withstand the evolving nature of those threats.

Chapter 2: Skimming in 2025 – Evolution of a Classic Con

Skimming is no longer about clunky overlays and card reader attachments. In 2025, it's a blend of micro-technology and wireless communication—designed to quietly extract value without disrupting customer experience or machine uptime.

The shift toward chip-based EMV transactions hasn't eliminated the problem; it's simply changed the attack vector. Fraudsters now deploy internal shimmers—razor-thin devices inserted inside the card reader—to intercept chip data. These are often paired with micro-cameras hidden inside the fascia or PIN pad to collect authentication credentials. Increasingly, these devices include Bluetooth and LTE modules, allowing criminals to exfiltrate data in real-time, without the need to ever return to the machine.

A notable case in late 2024 exposed just how widespread and coordinated this can be. Florida-based financial investigators uncovered a Romanian-led fraud ring responsible for outfitting over 400 retail ATMs across six states with LTE-equipped shimmers. The devices captured data continuously, which was transmitted to a central server abroad. The stolen data was used to clone cards and execute cash-outs at international locations, leading to an estimated $5.2 million in losses within a six-week period. [Source: Florida Department of Financial Services, Dec 2024]

Machines that lacked encrypted USB ports or routine inspection procedures were most vulnerable. And critically, most operators did not detect tampering until days or weeks after the devices were installed.

In response:

- **Genmega** introduced firmware 3.4.6+, which includes enhanced USB lockdown and stricter access controls.
- **Hyosung** released patch HS-R-2024-12, enabling administrators to disable vulnerable ports and upgrade communication protocols on Halo II and Force models.
- **Triton** issued guidance recommending deployment of Sentinel RMS and activation of encrypted Terminal Key Management (TKM) across all supported terminals.

The clear takeaway is that no single fix is sufficient. Operators need a layered defense approach—firmware, hardware, process, and training—that anticipates both device-based and software-based attack vectors.

Chapter 3: Jackpotting – A Heist Without a Mask

The term “jackpotting” may conjure images of movie-style heists, but the reality is far more systematic—and far more common. It refers to any attack that forces an ATM to dispense cash outside the bounds of legitimate transactions, typically using malware, external devices, or both.

In 2025, two dominant jackpotting methods are being exploited across North America:

- **Black Box Attacks:** Here, attackers open the top cabinet of an ATM, connect a device (often Raspberry Pi-based) directly to the dispenser port, and issue rogue commands that mimic legitimate instructions.
- **Malware Attacks:** These rely on injecting malicious code into the ATM’s operating system, often through USB drives or remote management tools. Once deployed, the malware allows attackers to initiate withdrawals or reset cash limits.

One high-profile case began unfolding in January 2025, when the U.S. Secret Service issued Bulletin #ATM-0125 in response to a wave of coordinated attacks spanning 11 states. The operation targeted Hyosung and Genmega terminals installed at retail locations with minimal physical safeguards. Attackers used black box kits—assembled for less than $100 in parts—and exploited exposed USB ports to trigger unauthorized dispensing. In total, financial losses exceeded $10 million in just five days.

OEMs responded swiftly:

- **Genmega's** Patchset 4.7.8 deployed encrypted communication protocols between the terminal's mainboard and the dispenser.
- **Hyosung** pushed secure boot processes and enhanced encryption in its MX8800 and MX8200Q series.
- **Diebold Nixdorf** expanded its Vynamic Security framework, emphasizing Trusted Secure Environments (TSEs) and application whitelisting for their DN Series ATMs.

More importantly, OEMs began recommending operational changes—like installing physical barriers, improving technician authentication, and conducting weekly audit logs for system access attempts.

Jackpotting is not an anomaly. It is a predictable attack model, and in many cases, a preventable one.

Chapter 4: ITM Loan Exploitation and Synthetic Identity Fraud

Interactive Teller Machines (ITMs) were designed to extend banking hours, increase convenience, and reduce in-branch volume. But as adoption grows, so do new opportunities for exploitation—especially in areas where human verification has been replaced by screen-based interactions.

A growing tactic in 2025 involves the fraudulent use of loan vehicles—particularly unsecured credit lines and home equity products—at ITMs. This is most often accomplished by combining synthetic identity profiles with gaps in remote teller workflows.

In one widely reported case, a regional bank in the Midwest identified more than $1.2 million in fraudulent disbursements across its ITM fleet. The attackers had used synthetic identities—manufactured from stolen Social Security numbers, false addresses, and fabricated credit profiles—to pass KYC protocols. Over a three-week period, they conducted over 70 transactions via video teller, drawing on approved credit lines without triggering red flags. [Source: FS-ISAC Threat Intelligence Brief, Q1 2025]

What made this particularly difficult to detect was the use of genuine credentials from different individuals, stitched together into believable identities. Verification questions were answered correctly. Session behavior appeared normal. And because teller workloads were high, none of the interactions were escalated.

The implications are clear: ITMs have become an unexpected entry point for sophisticated fraud schemes, particularly those exploiting instant access to credit. OEM and vendor response has begun to address this:

- **Hyosung** updated its MX8800 firmware in early 2025 to support biometric step-up authentication and improved logging of remote teller session metadata.
- **NCR** released a security bulletin outlining four-tier identity validation procedures and session flagging protocols for high-risk products.
- **Diebold Nixdorf** has begun piloting integration with third-party AML and behavioral monitoring software to flag outlier session patterns and identity inconsistencies in real-time.

Financial institutions are encouraged to treat ITMs not just as transaction endpoints, but as hybrid branches requiring the same level of layered security and fraud detection typically reserved for online and mobile banking channels.

Chapter 5: Remote Monitoring Software – Convenience vs. Control

Remote access tools are among the most useful assets in any technician's toolkit—but in recent months, they've also become one of the most frequently exploited vectors in ATM and ITM security incidents.

In their intended use case, Remote Monitoring and Management (RMM) platforms allow technicians to push updates, troubleshoot errors, and monitor uptime across large fleets. But when those tools are improperly configured—or worse, left exposed—they provide attackers with a direct pathway into the machine.

Several breaches in late 2024 and early 2025 confirmed this risk. In one case, a retail ATM deployer experienced a multi-day intrusion due to default credentials still active on a VNC session. In another, attackers used a compromised technician laptop to pivot into a network of more than 200 machines via an unpatched version of Netop. [Source: Dragos Security, RMM Risk Memo, Feb 2025]

In March 2025, Hyosung issued a formal technical bulletin warning customers about a specific attack targeting outdated versions of its MoniView RMS platform.

The bulletin detailed how criminals exploited known or default MoniView RMS passwords—or, when password validation wasn't enabled, pushed rogue configuration messages to older ATMs running BlueVerse Embedded (WinCE). This allowed network reconfiguration and opened the door for jackpotting attacks via man-in-the-middle tactics.

Hyosung's recommendations were clear:

- Upgrade to **BlueVerse Fleet Lite (MoniView) version 25.1.1**
- Change RMS passwords at the terminal level and avoid uniform credentials
- Enable password validation on all RMS servers
- Block incoming ATM registrations unless explicitly authorized
- Restrict inbound RMS traffic by IP or geography
- Use TLS encryption and limit firewall exposure to port 9999/9998 only

Source: Hyosung Technical Bulletin – RMS Attack, March 26, 2025

Even some financial institutions have faced challenges with internally managed RMM tools. One community bank in the Southeast acknowledged that an outdated version of TeamViewer, installed years earlier to troubleshoot an isolated performance issue, had remained active and unmonitored across their ITM fleet.

OEMs have taken notice:

- **Hyosung** issued a January 2025 memo directing all partners to discontinue use of TeamViewer in favor of encrypted VPN-based RMS.
- **NCR** reaffirmed in their Q1 2025 bulletin that all remote access should occur via zero-trust endpoints secured by hardware tokens and IP whitelisting.
- **Genmega** released new security documentation requiring local port lockdown for any machine running third-party remote access applications.

RMM tools aren't inherently unsafe—but they demand the same governance, credential hygiene, and update cadence as any other endpoint security platform.

Financial institutions and deployers should conduct a full audit of remote access practices and inventory every external-facing service in use. Because for every convenience gained through remote management, there's a potential cost in exposure—if not managed with precision.

Chapter 6: OEM Strategies and Responses – A Divided Landscape

The response to rising threats in the ATM and ITM space has not been monolithic. Each

OEM—whether focused on the retail market or serving financial institutions—has adopted its own approach, shaped by its platform architecture, client base, and internal risk posture.

For this reason, it's essential to separate OEM strategy into two distinct categories: **Retail ATM OEMs**, which prioritize volume deployment, affordability, and compact design, and **FI ATM/ITM OEMs**, which build for deeper integrations, larger footprints, and high-availability branch environments.

Retail ATM OEMs

Hyosung Retail Division (Halo II, Force) Hyosung holds a dominant 60–70% share of the U.S. retail ATM market, with its Halo II and Force series deployed at thousands of off-premise locations. Though better known in the FI sector, its presence in retail is deep and influential.

- In late 2024, Hyosung issued Patch HS-R-2024-12, addressing USB vulnerabilities and providing tools to enforce encrypted data transfer between components.
- The company now requires all new Halo II and Force deployments to use upgraded cabinet locks and to implement software authentication for dispenser control.
- Partners are being encouraged to migrate to Hyosung RMS in lieu of public RMM utilities.

Genmega is the second-largest retail ATM OEM in the U.S., with a significant footprint in convenience stores, gas stations, and independent retail locations. Recent incidents involving black-box jackpotting and shimmer-based skimming have prompted Genmega to strengthen its defensive posture.

- In January 2025, Genmega released **firmware version 4.7.8**, enabling encrypted communication between the terminal's processor and dispenser.
- Additional advisories urged operators to disable USB access and remove unused RMM tools, particularly VNC and legacy Netop installations.
- Genmega's **Security Center** now includes downloadable physical security guides for retail deployers.

Genmega's architecture remains relatively open, which offers IADs operational flexibility—but that flexibility must be paired with disciplined security practices. Proper configuration, regular audits, and prompt patching are essential to fully securing Genmega deployments.

Triton's position in the U.S. market is smaller but long-standing, with strong penetration in off-premise deployments.

- Triton recommends deploying **Sentinel RMS**, its proprietary monitoring tool, alongside **XScale firmware** which includes anti-jackpotting logic.
- Their 2025 guidance emphasizes the importance of physical USB lockout kits and encrypted Terminal Key Management (TKM).
- Triton continues to provide customer-specific patch guidance and urges operators to disable unused network ports and conduct physical inspections during each cash load cycle.

(Halo II, Force)** While Hyosung is widely recognized for its FI solutions, its retail division serves a substantial U.S. market.

- In late 2024, Hyosung issued **Patch HS-R-2024-12**, addressing USB vulnerabilities and providing tools to enforce encrypted data transfer between components.
- The company now requires all new Halo II and Force deployments to use upgraded cabinet locks and to implement software authentication for dispenser control.
- Partners are being encouraged to migrate to **Hyosung RMS** in lieu of public RMM utilities.

FI ATM and ITM OEMs

Hyosung FI Division Hyosung's MX series has gained popularity among credit unions and mid-sized banks, particularly for ITM applications. The company has responded aggressively to recent fraud cases:

- In February 2025, firmware updates across the **MX8800 and MX8200Q** platforms included enhanced session logging, secure boot features, and stronger encryption between the CPU and cash dispenser.
- Hyosung also issued new standards for ITM video session authentication, urging the use of biometric step-up verification for credit product access.
- A network-wide RMS update mandates two-factor authentication for technician access.

NCR With a legacy customer base and a reputation for stability in the FI market, NCR has focused on building layered defenses tied to its software ecosystem.

- NCR recommends enabling **Solidcore Suite**, which enforces application whitelisting and secure OS controls on all SelfServ and Activate machines.
- In 2025, NCR published guidance on session-layer encryption, urging operators to migrate from Windows 7/10 to hardened Linux or Windows IoT deployments.
- Remote access, when permitted, must be routed through NCR's Secure Access Gateway with IP whitelisting, device fingerprinting, and endpoint encryption.

Diebold Nixdorf Diebold Nixdorf's response has centered on platform hardening and ecosystem integration through Vynamic Security, which combines hardware, software, and behavioral analytics.

- The **DN Series** now ships with Trusted Secure Environment (TSE) technology, leveraging a secure enclave within the ATM's architecture.
- Diebold encourages integration with third-party fraud detection systems for ITM deployments, including behavioral biometrics and session anomaly detection.
- They have also promoted partnerships with cybersecurity firms to provide **zero-trust security audits** for existing FI customers.

The OEM landscape is shifting—gradually but deliberately. Those offering prescriptive, vertically integrated solutions are gaining favor among financial institutions, while retail-oriented OEMs continue to balance flexibility with the need for stronger defaults.

For all deployers, the essential task remains the same: to actively engage with OEM bulletins, implement layered defenses, and ensure that service partners are operating to the latest configuration and firmware standards.

Chapter 7: What Institutions and Deployers Should Do Next

Understanding the threat landscape is one thing. Acting on it is another. The security events of the past 18 months—documented by FS-ISAC, Secret Service, and OEM security teams—make one thing clear: the institutions and deployers that remain passive or rely solely on vendor defaults are at greater risk.

The most successful responses to these threats have come from institutions and operators that treated ATM and ITM security as an enterprise risk—not just a technical one.

---

1. Conduct a Full Asset Inventory and Risk Audit

Before making any changes, understand what you're working with:

- Which models do you have deployed? Are they running current firmware?
- What remote tools are in use (e.g., Netop, TeamViewer, RMS)?
- Who has access to physical keys or RMM credentials?

In 2024, a community bank in Tennessee discovered multiple unauthorized RMS installs across its ITM fleet during a vendor transition audit. The software had been installed years prior and never decommissioned, despite staff turnover. No breach occurred—but the exposure was real, and avoidable.

Action: Use the FS-ISAC ATM Risk Checklist (2025 update) as a starting point. [FS-ISAC Members Only, March 2025]

---

2. Patch and Lock Down USB and Network Ports

Every jackpotting event cited in USSS Bulletin #ATM-0125 involved unsecured USB or network access. Most occurred at night or over weekends when response teams were slower.

Action: Implement OEM-specific physical and logical port lockout protocols. For example:

- Genmega firmware 4.7.8
- Hyosung Patch HS-R-2024-12
- Triton's USB blocker kits (2025 bulletin)

Source: U.S. Secret Service Field Alert #ATM-0125 (January 2025)

---

3. Segment and Secure RMM Access

Many recent breaches stemmed not from the ATMs themselves, but from weak links in remote access infrastructure.

In 2025, a regional ISO in the Midwest suffered a breach where VNC access credentials were stolen from a technician's laptop that lacked endpoint detection software. Attackers used this entry point to monitor—and eventually control—over 150 ATMs remotely. Law enforcement is still investigating.

That same month, **Hyosung confirmed an RMS-targeted exploit** that used default or unvalidated MoniView credentials to push rogue ATM configurations. Older versions of BlueVerse Embedded (WinCE) were especially vulnerable to reprogramming that allowed jackpotting attacks over the network. [Source: Hyosung Technical Bulletin – RMS Attack, March 26, 2025]

Action:

- Eliminate shared logins for RMM tools
- Require multi-factor authentication for all remote access
- Upgrade to BlueVerse 25.1.1 and enforce password validation on RMS servers
- Restrict inbound RMS traffic to known ATM IPs or regions

Source: Hyosung RMS Security Guidance + Dragos Security Brief (Feb–Mar 2025)

4. Strengthen ITM Credit Access Controls

The synthetic identity exploitation of ITMs revealed a major gap in identity verification. Institutions should treat high-risk transactions on ITMs as they would online or mobile banking fraud.

Action:

- Require dual verification for unsecured loan draws
- Flag first-time video sessions drawing from credit lines
- Review teller session logs weekly for behavioral anomalies

In one confirmed FS-ISAC case, a Northeast credit union recovered losses only after forensic video review revealed pattern behavior across multiple ITMs from different IP addresses using similarly structured synthetic profiles.

Source: FS-ISAC Synthetic Identity Exploits Brief (March 2025)

---

5. Align Vendors to a Formal Security SLA

Whether it's your core processor, armored carrier, or field technician partner—make sure everyone plays by the same security standards.

Action:

- Update contracts to require firmware updates within 30 days of OEM release
- Require RMS logs and access audits quarterly
- Hold vendors accountable to your institution's risk standards, not just theirs

Too many breaches stem from a breakdown in vendor expectations. A formal SLA can close that gap.

Security isn't just about reacting to incidents—it's about resilience. Institutions that survived the 2024–25 fraud wave with minimal losses weren't lucky. They were prepared, vigilant, and intentional.

There is no silver bullet. But there is a proven path—and it starts with ownership, visibility, and disciplined execution.

Chapter 8: The Road Ahead – Collaborating to Stay Ahead of Threats

As fraud tactics become more sophisticated, the burden of ATM and ITM security must be shared—not siloed. No single institution, deployer, or OEM can solve this alone.

The financial ecosystem's resilience will depend on ongoing collaboration, intelligence sharing, and strategic alignment across the industry. What comes next isn't about responding faster. It's about designing systems, partnerships, and processes that make your fleet harder to compromise in the first place.

Know Your Segment – and Elevate Your Standards Accordingly

The threat profiles for retail and FI environments differ, but both require modernization:

- **Retail ATM Deployers:** Hyosung occupies an estimated 60–70% of the U.S. retail ATM market, with its Halo II and Force models being the most widely deployed off-premise terminals. Their RMS platform, BlueVerse, and associated security bulletins should be considered essential infrastructure—not optional updates. Genmega, the second-largest player in retail, has taken meaningful steps with firmware version 4.7.8 and encrypted USB communication between critical components. While its architecture offers operators greater flexibility, that openness demands strong operational discipline. Triton, though smaller in share, continues to support its footprint with Sentinel RMS and XScale firmware—providing valuable security tools to those willing to implement them diligently.

Don't treat "off-premise" as off-the-hook. These machines process real customer data and dispense real cash. Standards should reflect that. These machines process real customer data and dispense real cash. Standards should reflect that.

- **Financial Institutions:** The future of ITMs hinges on maintaining customer trust. As devices grow more complex, with video integration and real-time loan access, institutions must treat ITM authentication, identity resolution, and session monitoring as primary controls—not as secondary protections.

Most successful fraud attempts didn't break systems—they bypassed weak processes. The next generation of security will rely on AI-enhanced anomaly detection, biometric step-up verification, and hybrid teller oversight.

Join—and Contribute to—Information-Sharing Communities

Platforms like FS-ISAC, ATMIA's new Security & Risk Committee, and regional law enforcement working groups offer valuable, real-time threat intel. But the benefit is mutual—institutions that report emerging tactics help shape industry response.

- Participate in monthly FS-ISAC ATM Security Threat Exchange (STEX) calls.
- Submit redacted fraud incident summaries to ATMIA's confidential bulletin archive.
- Encourage state banking associations to hold joint sessions with law enforcement and OEMs.

Fraud evolves too quickly for competitors to operate in isolation.

Demand More From Vendors—Upstream and Downstream

Security is a chain of custody. If your armored carrier is leaving terminals unlocked for minutes or your RMS vendor is recycling credentials, your controls are already compromised.

- Enforce credential expiration across RMM platforms.
- Require OEM patch deployment within 30 days—no exceptions.
- Audit technician behavior during site visits—then rotate access keys every quarter.

This is no longer just about compliance. It's about viability.

Invest in Training and Culture—Not Just Technology

Fraud prevention tools are only effective when people understand how to use them. Make frontline staff and third-party techs your first layer of defense.

- Provide ATM fraud recognition training annually.
- Include ATM/ITM threat simulation exercises in IT incident response plans.
- Update internal documentation after every incident, not just quarterly reviews.

Technicians, call center staff, and even branch personnel can become early warning systems—if you equip them.

Final Thought

We're entering an era where ATM and ITM security cannot be treated as a niche responsibility. It's brand defense. It's risk management. It's customer protection.

The next attack is already in motion. But so is your response. Choose to be proactive, informed, and aligned—and you won't just mitigate risk. You'll lead the industry.

Works Cited

Fischer, Carsten. “The Need for Speed in Threat Mitigation.” Carsten Fischer, www.fsisac.com/insights/podcast/carsten-fischer-the-need-for-speed-in-threat-mitigation. Accessed 31 Mar. 2025.

Holder, Hannah. “Secret Service Issues Public Advisory on ATM Skimming.” Texas Bankers Association, 6 Mar. 2025, www.texasbankers.com/secret-service-issues-public-advisory-on-atm-skimming/.

Publisher. “Hyosung and Genmega Recommend Actions to Protect Your Atms.” ATM Biz Center - ATM Industry News & Resource Center, 23 Aug. 2024, atmbizcenter.org/blog/hyosung-and-genmega-recommend-actions-to-protect-your-atms/.

“2025 OT Cybersecurity Report.” Dragos, 1 Jan. 2024, www.dragos.com/ot-cybersecurity-year-in-review/.

“ATM & POS Terminal Skimming.” ATM & Pos Terminal Skimming, www.secretservice.gov/investigations/skimming. Accessed 31 Mar. 2025.

“The State of Synthetic Fraud: Evolution, Trends, and How We Will Eradicate It By 2026.” Socure, socure.drift.click/state-of-synthetic-fraud. Accessed 31 Mar. 2025.