NCR ATLEOS | Trellix

Securing the Modern Banking Ecosystem – Part 1

From Physical Threats to AI-Enabled Fraud:

Concerns and Solutions for Financial Institutions

July 2026

NCR ATLEOS | Trellix

July 2026

From Physical Threats to AI-Enabled Fraud:

Concerns and Solutions for Financial Institutions

Table of contents

Executive summary

Banks and ATM deployers face a convergence of physical crime, AI-driven social engineering, supply-chain fragility, as well as governance and behavioral gaps. The security landscape for Financial Institutions remains volatile and at times challenging.

In March NCR Atleos and Trellix joined forces to host our first security summit at Abertay University Cyber Quarter in Dundee. By bringing together industry security experts, Financial Institutions, and experts in cyber and fraud academia we collectively asked questions and discussed real-time challenges on how to stay ahead of fraud and cyber-attacks both aimed at the banking industry and beyond. We highlighted reporting frictions (e.g. data-sharing concerns under GDPR), over-reliance on reactive controls, and complex incidents that can often stretch resources for lengthy periods of time.

In the first whitepaper, we look at two specific areas around trust and threats.

Trust & Threats The Shift in Physical Attacks Responsible Finance	**Operational Resilience** Disaster Recovery Supply Chain Security
Securing Tomorrow AI Driven Phishing & Social Engineering Evolving Attack Vectors	**Covert & Coercive** Risk Management Governance & Human Behavior

Physical ATM attacks: trends, impact and emerging risk dynamics

Despite an overall decline in the volume of physical ATM attacks across Europe in 2025, the financial and operational impact of such incidents continued to intensify. Data from EAST (European Association for Secure Transactions) highlights a shift in both attacker behavior and the economic consequences of these crimes, reinforcing the need for financial institutions to reassess physical security strategies alongside evolving fraud vectors.

Declining incident volumes mask growing financial impact

EAST reports that total ATM-related physical attacks fell by 50% year-on-year, decreasing from 5,593 incidents in 2024 to 2,986 in 2025. This reduction was largely driven by a 60% drop in non-specific attack categories, suggesting either improved classification or a genuine decline in opportunistic or lower-sophistication attacks.

However, this positive trend is offset by a sharp increase in total losses, which rose 58% to €19 million (up from €12 million in 2024). This divergence between incident volume and financial impact indicates that attackers are becoming more targeted, more effective, or are focusing on higher-value ATM locations.

Explosive attacks continue to drive losses

Explosive attacks remain the most significant contributor to financial losses:

- Incidents decreased slightly by 6% (from 602 to 565 cases)
- Losses increased by 57%, rising from €8.6 million to €13.5 million
- These attacks account for 71% of all physical ATM-related losses

This trend underscores a critical shift: fewer attacks, but greater success rates and higher-value outcomes. It also highlights the increasing sophistication and organization of criminal groups deploying explosive methods, often targeting high-cash-volume ATMs or sites with weaker physical protection.

Importantly, EAST notes that approximately 40% of explosive attacks do not result in cash loss, yet the reported figures exclude collateral damage. In practice, damage to ATM units, surrounding infrastructure, and buildings can significantly exceed the value of stolen cash, amplifying the total cost of ownership and operational disruption for financial institutions.

Other physical attack vectors

Beyond explosive incidents, other categories show moderate declines:

- **ATM theft (rip-out) and burglary (in-situ):** Down 11%, from 592 to 525 incidents
- **Non-specific physical attacks:** Down sharply by 60%, from 4,754 to 1,889 incidents

While these declines suggest improved preventative measures—such as enhanced anchoring, ATM placement strategies, and surveillance, they should not be interpreted as a reduced threat. Rather, they reflect an evolution toward more specialized and higher-return attack methodologies.

Strategic implications for financial institutions

1. Shift from volume- to severity-based risk management

Traditional metrics focused on attack frequency are no longer sufficient.
The disproportionate increase in losses related to incidents highlights the need for:

- Risk models that prioritize potential financial impact per location
- Enhanced protection for high-risk, high-cash ATMs
- Geographic risk profiling based on organized crime activity

2. Increased importance of physical hardening

Given the dominance of explosive attacks, institutions should prioritize:

- Anti-explosive ATM technologies (e.g. ink dye systems, gas neutralization)
- Reinforced ATM safes and secure anchoring solutions
- Strategic placement in controlled or monitored environments

3. Total cost of attack consideration

Financial institutions must adopt a broader cost perspective that includes:

- Property and infrastructure damage
- ATM downtime and service disruption
- Reputational impact and customer trust erosion

These are particularly relevant given that reported loss figures exclude collateral damage, which can exceed direct cash losses in many cases.

4. Integration with wider security strategy

Physical ATM attacks should not be viewed in isolation. The wider EAST report indicates a surge in advanced fraud methods, particularly data relay attacks, which reinforces the need for:

- Integrated fraud and physical security frameworks
- Cross-channel threat intelligence sharing
- Collaboration with law enforcement and industry bodies such as EAST and Europol

Accessibility of advanced breaching tools

The widespread availability of formerly specialist tools has dramatically lowered the barrier to entry for ATM attackers. Equipment such as the Jaws of Life, once dependent on vehicle mounted compressors, is now available in **handheld consumer variants**, purchasable online or in some cases stolen from unmanned fire stations.

This evolution enables criminals to:

- Complete breaches in **under six minutes**
- Target ATMs holding **€80,000 – €£90,000** in cash
- Operate with less training and fewer resources

As tools become smaller, more powerful, and easier to acquire, physical attacks increasingly resemble high-speed, high-precision operations.

Influence of economic and criminal justice factors

Cost of living pressures

Economic hardship remains a significant macro-level contributor to acquisitive crime. This environment lowers deterrence thresholds for both opportunistic and organized offenders.

Early release dynamics

Early release schemes have accelerated the return of experienced offenders to criminal markets, reinforcing longstanding physical attack methods.

Return to "traditional" crime

Digital crime carries an increasing forensic footprint; many criminals are shifting back to well understood, lower traceability physical crimes such as ATM attacks.

Organized criminal activity and evolving tactics

While opportunistic offenders continue to attempt copycat attacks, the majority of successful physical ATM breaches exhibit clear signs of organization:

- Multi-country criminal networks responsible for **millions in losses** were dismantled by Europol in 2024, highlighting the cross-border nature of modern ATM crime
- Gangs increasingly employ solid explosives sourced from **heavy pyrotechnics**, heightening risk and collateral damage to buildings and residents
- Coordinated reconnaissance, targeted attacks, and high-powered getaway vehicles are now routine

In 2025, another sophisticated group was arrested after a series of explosive ATM heists across Austria, Germany, and the Netherlands, using flash powder devices and precise scouting of vulnerable ATM sites.

These operations demonstrate escalating professionalism and international coordination.

Surge in terminal fraud and lower payout attacks

Beyond physical breaches, Europe saw a dramatic rise in smaller, high-volume fraud attacks:

- Terminal fraud incidents rose from **7,115 cases in 2023 to 14,664 in 2024**—a 106% increase
- Despite more incidents, losses dropped from **€173M to €71M**, reflecting improved cybersecurity and fraud prevention controls
- Cash trapping attacks fell **33%** (7,166 → 4,795) and relay attacks dropped **87%** (502 → 63)

Criminal tactics are clearly shifting toward less risky, higher frequency attacks that collectively yield substantial returns.

Additionally, a UK–Romanian organized crime group used Transaction Reversal Fraud (TRF) to steal **€580,000**, demonstrating the continued evolution of fraud-based methodologies.

Information sharing barriers and GDPR constraints

A recurring theme among law enforcement and financial industry stakeholders is the restrictive impact of GDPR on intelligence sharing:

- Banks often withhold essential data due to fear of regulatory penalties
- Investigations stall without shared forensic evidence
- Cross organizational collaboration is weaker despite shared goals

With attack volumes rising, current regulatory frameworks increasingly inhibit timely, coordinated responses.

In conclusion

ATM crime is entering a new phase defined by:

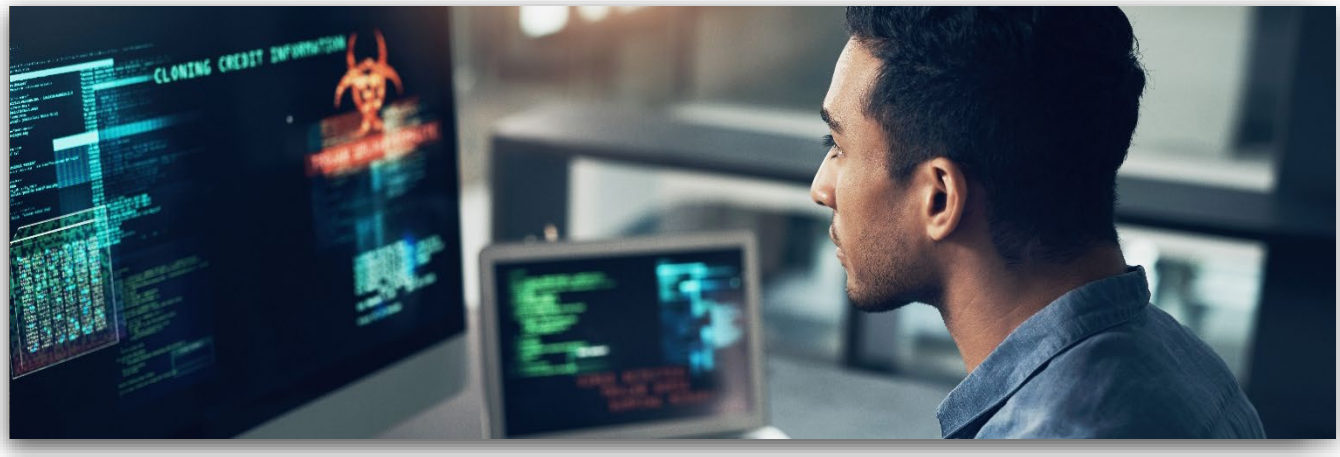
- Higher incident volumes
- Faster and more destructive physical attacks
- An increasing role for cross-border organized networks
- Greater accessibility of advanced breaching tools
- Regulatory hurdles that limit collective response

Although financial losses have decreased due to improved protections, the **overall threat level is rising**, with criminals adapting faster than regulatory or organizational frameworks.

The industry must now prioritize:

- Strengthened intelligence sharing
- Mechanical hardening of ATM infrastructure
- Modernized regulations to enable safe data exchange
- Enhanced law enforcement collaboration
- Investment in rapid response technologies

ATM crime prevention is no longer a technical challenge alone—it is an ecosystem challenge requiring integrated action across public, private, and regulatory domains.



Responsible finance

The rapid digitization of financial services has transformed consumer behavior, accelerated innovation, and reshaped payment ecosystems. Yet the transformation presents significant challenges, particularly around digital exclusion, biometric risk, consumer vulnerability, and inconsistent industry reporting.

The next section explores those challenges and identifies the collaborative, regulatory, and educational interventions needed to support a more responsible financial future.

The new digital financial landscape—from physical cash to invisible payments

For decades, cash provided a tangible, intuitive anchor for personal financial management. Today, consumers navigate fully digital payment environments—many starting as young as 16 if not younger — while others, including older adults, struggle with digital tools that feel unfamiliar or intimidating.

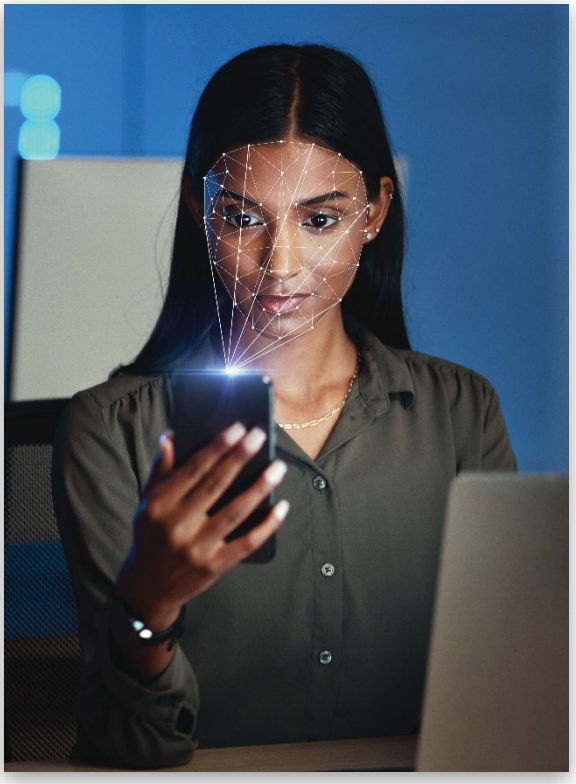
The shift to digital accelerated sharply during COVID-19 as retailers moved away from cash. Millions were pushed into digital payments earlier than expected, creating a divide between digitally fluent consumers and those who remain uncertain or excluded. However, the group were quick to highlight that it's not just the older generation who face challenges. The span is ranging, from teenagers buying on their phones to people who struggle with mobile phones.

Biometric authentication: convenience vs. confidence

Biometric authentication (face ID, fingerprint scanning) has redefined digital identity verification and payment approval. It offers unmatched convenience — but also introduces risks consumers may not yet understand.

Key concerns include:

- Irrevocability of compromised biometrics
- Data governance and ownership
- Challenges in explaining biometric risk to consumers
- Growing reliance on private technology platforms
- Reluctance of organizations to “own” biometric repositories due to regulatory challenges, cost, and practical management requirements.



Responsible finance requires ensuring that a technology designed to enhance security does not inadvertently create new forms of vulnerability.

Digital exclusion: a hidden vulnerability

Many consumers lack confidence in digital interfaces and rely on others to manage their financial tasks.

This introduces:

- **Dependency** — relatives or caregivers become intermediaries
- **Exposure** — increased risk of scams, coercion, or errors
- **Confusion** — uncertainty about what is legitimate or safe

The industry must recognize that digital exclusion affects not only older adults but also individuals with limited access, literacy, or experience navigating digital systems.

Regulations, reimbursements, and moral hazard

Regulation requires banks to reimburse customers who fall victim to fraud, offering essential consumer protection. Yet this introduces a **moral hazard dilemma**:

- If consumers assume banks will always refund losses, risk-taking may increase.
- Banks argue this undermines personal responsibility and increases systemic costs.
- Regulators emphasize protection in an environment where fraud evolves rapidly.

Finding the balance between accountability and protection is central to a responsible, resilient financial ecosystem.

Transparency gaps and reporting inconsistencies

Fraud and incident reporting vary dramatically across organizations. Some institutions report comprehensively; others report only what is mandatory; smaller firms often fear reputational damage.

This creates:

- Fragmented national data
- Hidden systemic vulnerabilities
- Poor cross-industry learning
- Unclear fraud trends

A more responsible system requires **mandatory, standardized reporting** and proactive data-sharing across the sector.

The debate around digital identity

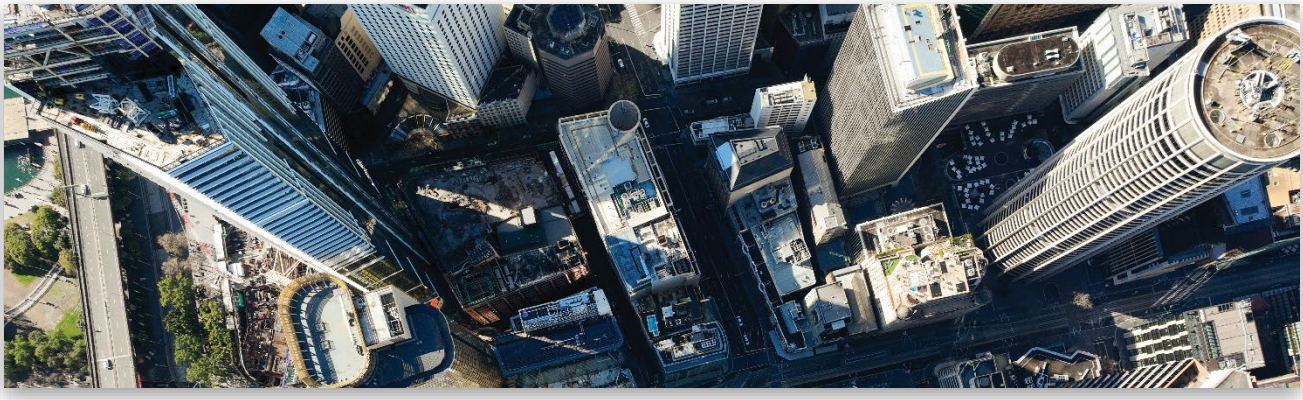
Digital ID systems offer efficiency, fraud reduction, and streamlined public services. Countries like Estonia and the Netherlands have demonstrated their value. However, cultural resistance — particularly around state surveillance, concerns — presents adoption challenges.

Successful implementation would require:

- A national public information campaign
- Strong privacy protections
- Clear explanation of personal benefits
- Trust-building across all demographics

Digital ID may offer transformative benefits, but only with public trust as its foundation.

Strategic recommendations



Industry recommendations

- **Adopt universal fraud reporting standards**
  Ensure incident transparency across all financial institutions, regardless of size.
- **Design for accessibility**
  Simplify user interfaces, reduce cognitive load, and embed inclusive design principles.
- **Increase cross sector collaboration**
  Establish ongoing networks between banks, retailers, regulators, and technology providers.
- **Strengthen consumer communication on biometric risk**
  Provide simple, clear explanations and safeguards around biometric use.

Regulatory recommendations

- **Mandate consistent and timely fraud reporting**
  Build a unified national database that reveals emerging trends.
- **Enhance digital ID governance frameworks**
  Provide clear privacy, data use, and protection standards before launch.
- **Implement targeted education campaigns**
  Focus on digitally excluded groups, including older adults and vulnerable communities.
- **Balance reimbursement rules with consumer responsibility**
  Encourage secure behavior without penalizing vulnerable groups.

Consumer support recommendations

- **Introduce “digital confidence” training programs**
  Delivered through banks, retailers, and community partners.
- **Make fraud risk indicators more visible**
  Simple warnings, mandatory delays, or contextual explanations on risky transactions.
- **Provide trusted pathways for support**
  Reduce reliance on family members by offering verified helpers or secure assistance channels.

In conclusion

Responsible finance in a digital world requires balancing innovation with accessibility, safety with convenience, and individual responsibility with consumer protection. The conversation captured in the transcript highlights the need for industry-wide collaboration, better public education, stronger reporting systems, and cultural sensitivity when introducing new technologies such as digital ID.

By acting collectively, the financial sector can build a resilient, inclusive, and trustworthy digital ecosystem that supports all consumers — not just digitally fluent.

"It's not just the older generation who face challenges, the span is vast, from teenagers buying on their phones to people who struggle with mobile phones."

Scott Millar
Tesco Insurance & Money Services

Final summary

The series of whitepapers highlight how financial institutions are facing a rapid convergence of physical ATM attacks, AI-enabled social engineering, and growing governance and human-behavior challenges, all intensified by regulatory and intelligence-sharing barriers. It argues that rising threat sophistication demands a shift toward ecosystem-wide collaboration, earlier security integration, and human-centered governance to build long-term resilience. Ultimately, securing the modern banking landscape requires coordinated action across technology, regulation, and culture.

NCR Atleos and Trellix would like to thank everyone who took part in the cyber summit sessions, for their willingness to participate, contribute, and collaborate so openly throughout the discussions.