VISA

Spring 2026 Biannual Threats Report

A strategic perspective on payment security

Visa Network Defense

A Note from Paul Fabara

Chief Risk and Client Services Officer

Fraud is an ongoing battle between defenders and adversaries. As defenses strengthen in one area, attackers often redirect to less-defended surfaces, often not infrastructure, but people.

Over the last six months, Visa blocked a **13% increase in unique enumeration attacks** at the network level while continuing to deliver measurable improvements in core security outcomes—clear evidence that network scale defenses are working.

But while security initiatives are working, the nature of the threat is changing as fraudsters are moving their targets. Scams have become the fastest growing consumer risk, increasingly enabled by sophisticated impersonation and AI driven social engineering. Fraud is increasingly a problem of **behavioral manipulation, ecosystem fragmentation, and accelerated attack cycles enabled by AI**.

Staying ahead now requires more than incremental control improvements. It requires a **shared, system-level approach to security** across all points of the financial ecosystem: financial institutions, merchants, technology platforms, and policymakers. Resilience is only as strong as the system in which all participants operate.

This report outlines the structural shifts reshaping payment security and what they mean for leaders responsible for protecting trust in digital commerce.

Paul Fabara
Chief Risk and Client Services Officer

Executive Summary

The nature of fraud is shifting from technical compromise to behavioral manipulation, forcing a structural redefinition of how payment security must operate.

Improvements in authentication, increased tokenization adoption, and enhanced network-level defenses are mitigating traditional fraud vectors. But as these controls strengthen, adversaries are rapidly shifting towards less-defended surfaces – people, processes, and third-party integrations – often using AI to scale deception and to accelerate attack cycles.

Across the second half of 2025, four shifts demonstrated this global shift in payment security:

Foundational controls continue to improve outcomes even as attack volumes rise

Scams have become the primary source of consumer harm

AI is accelerating both attack and defense

Ransomware remains prevalent, but the economics of payment are changing

As a result, organizations need to complement transaction-level fraud detection with ecosystem-level management, where speed, coordination, and AI-enabled anomaly detection become critical defenses.

What the data shows

- **Core security is improving.** Device-token fraud declined **9.6% year over year**, while losses tied to enumeration declined **16%**, largely due to the tens of millions of suspected fraud blocked by Visa's Risk Operation Center.
- **Scams are now a primary threat.** Nearly **$1 billion** in scam related fraud attempts was identified between July and December 2025.
- **AI is reshaping both attack and defense.** Criminals are using AI to scale scams and automate attack workflows, while defenders, including Visa, are increasingly using AI to stop attacks earlier and mitigate losses.
- **Ransomware: more attacks, less payment.** Global ransomware activity rose **26% in July 2025-December 2025 over the same period in 2024**, but a mere **23%** of victims paid ransoms, the lowest rate on record. These declines can be attributed to many organizations' reluctance to paying ransoms, as victims have learned paying has little effect on whether their sensitive data is leaked to the public.

What it means

- **Security failures increasingly occur at ecosystem seams.** The most consequential failures increasingly occur at boundaries between institutions where incentives and visibility are misaligned.
- **Fraud is no longer primarily a credential problem – it is a behavioral problem.** As authentication improves, adversaries increasingly convince legitimate users to authorize illegitimate transactions, forcing a shift from "detect stolen credentials" to "detect and disrupt deception."
- **AI makes speed even more of a competitive advantage in defense.** Defensive models built around manual review and slow moving patterns underperform against adversaries operating at machine speed.
- **Resilience matters as much as prevention.** With ransomware activity rising but payment rates declining, business continuity and recovery must be treated as primary security controls instead of afterthoughts.

The Strategic Threat Landscape: Four Shifts Reshaping Payment Security

SHIFT #1

Security is working, but attackers are reallocating effort

The payments ecosystem has made meaningful progress. Even as attack activity rises, improvements in tokenization, authentication, and network level detection are delivering measurable results. Token fraud declined **9.6% in July – Dec 2025 over the same period in 2024**, while enumeration losses declined 1**6%** during the same period.

Implication:

Success in core controls does not mean risk is shrinking. It means adversaries are moving toward less defended surfaces like people and third party dependencies. This requires shifting from lagging indicators (fraud losses) to forward-looking signals of where fraud is moving next. The most important question is no longer "how much fraud occurred," but "where is fraud migrating – and how quickly?" Consequently, the focus will be on ecosystem-level vulnerabilities, third-party dependencies, and process and configuration gaps.

Strategic Considerations for Executives:

- ✓ Reorient performance metrics towards risk migration, not just loss reduction by tracking where attempts and losses are shifting across channels, use cases, and jurisdictions.
- ✓ Prioritize controls at the seams: merchant onboarding controls, platform integrity, identity verification, and cross partner collaboration.
- ✓ Incorporate forward-looking threat intelligence and analysis as a core fraud operations function.

SHIFT #2

Scams are the dominant consumer threat

Scams are now the largest and fastest growing category of consumer fraud. From July–December 2025, **nearly $1 billion** in scam activity was identified. AI is accelerating this shift by enabling threat actors to scale and refine deceptive tactics. The use of AI generated content, voice impersonation, and deepfake media can increase both the reach and perceived credibility of scams when exploited by actors with malicious intent.

Implication:

Scam prevention cannot be solved solely with controls at the authorization layer. When the user behaves "legitimately" from a transaction perspective, scam defense becomes a combined challenge of identity verification, intent assessment, and manipulation detection—often requiring coordinated action beyond a single institution.

Strategic Considerations for Executives:

- ✓ Build deception defense capabilities aimed at identifying impersonation patterns, scam merchant ecosystems, and higher risk funnels (search, ads, social, etc.).
- ✓ Treat customer communications as a security control, emphasizing trusted channels, verified identity, and clearly defined guardrails for customer interactions.
- ✓ Align incentives and escalation paths across ecosystem partners to support faster takedown efforts of scam networks.

The Strategic Threat Landscape: Four Shifts Reshaping Payment Security

SHIFT #3

AI is compressing the fraud cycle (for attackers and defenders)

AI is transforming both sides of the fraud equation. Attackers use AI to generate highly personalized and convincing scams, automate workflows at scale, and rapidly iterate and adapt tactics. Defenders use AI to detect anomalies earlier, stop attacks before they reach consumers or merchants, and improve detection precision.

The strategic shift is speed. Attacks iterate faster, scale faster, and adapt faster. In ransomware, AI tools have compressed attack timelines from days to minutes.

Implication:

Organizations that rely on manual, siloed review models are structurally disadvantaged. The advantage belongs to those that can act in real time, coordinate across partners quickly, and automate the detect-triage-response lifecycle.

Strategic Considerations for Executives:

- ✓ Modernize controls for machine speed: automation in detection, triage, and response; fewer handoffs; clearer authority to intervene quickly.
- ✓ Invest in authentication and verification methods resilient to synthetic audio, video, and highly tailored persuasion.
- ✓ Implement cross-partner response capabilities across key stakeholders for collaborative decisioning.

SHIFT #4

Ransomware is rising, but the economics are shifting

Ransomware incidents continue to increase (+26% July-December 2025 over the same period in 2024), but victims are paying less frequently (23% paid during the July-December 2025 period, the lowest rate on record) and paying less on average (down 66% from July to September 2025 over April-June 2025). This reflects improving resilience and growing recognition that paying does not reliably prevent data release.

Implication:

Ransomware is increasingly a resilience and recovery challenge—not just a prevention problem. Organizations that restore quickly and contain blast radius materially reduce both damage and attacker leverage.

Strategic Considerations for Executives:

- ✓ Treat recovery time objectives and backup integrity as board level metrics.
- ✓ Reduce third party blast radius through security standards, integration monitoring, and rapid notification requirements.

How Visa Helps — Defending the Payments Ecosystem at Scale

Protecting trust in digital payments requires action at scale and coordination across institutions and geographies. Visa plays a unique role in safeguarding the payments ecosystem by combining network level intelligence, real time defenses and ecosystem collaboration.

Visa protects the payments ecosystem through:

Real time transaction monitoring

Continuous, AI driven monitoring across the network to detect and block emerging threats—preventing fraud before it reaches consumers, merchants, or financial institutions.

Network level disruption of large-scale attacks

Centralized visibility enables Visa to identify coordinated, cross merchant and cross border attack patterns and apply protections at network scale—something no single institution can achieve alone.

Dedicated scam disruption capabilities

A specialized scam disruption team focused on identifying, investigating, and dismantling scam networks, uncovering nearly $1 billion in scam activity in just six months, and accelerating takedowns of fraudulent merchants and infrastructure.

Collaboration across the ecosystem

Ongoing coordination with banks, merchants, technology partners, and global law enforcement agencies to disrupt criminal networks tied to millions of victims worldwide, reducing repeat attacks and limiting the spread of harm.

Selected Metrics & Definitions (Methodology excerpt)

This executive edition reflects observations across the second half of 2025, including network-level attack blocking, scam identification activity, and ransomware trend monitoring. Key indicators include token fraud trends, enumeration loss trends, enumeration blocking volumes, scam activity identified July–December 2025, and ransomware incident and payment trends.