VISA

Biannual Threats Report

Five Forces Reshaping Payment Security in 2025

A Payment Ecosystem Report by
Visa Payment Ecosystem Risk and Control

Fall 2025

Table of Contents

Executive Overview

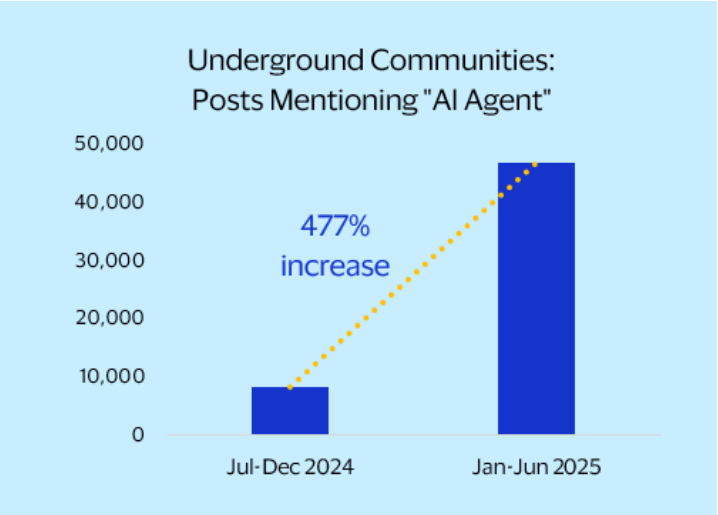
The global payments ecosystem is experiencing a fundamental shift in how fraud operates. In the first half of 2025, Visa's Payment Ecosystem Risk and Control (PERC) team identified five transformative patterns that cut across traditional threat categories — patterns that reveal how criminals are adapting faster, operating at greater scale, and exploiting structural vulnerabilities in ways that challenge conventional defenses.

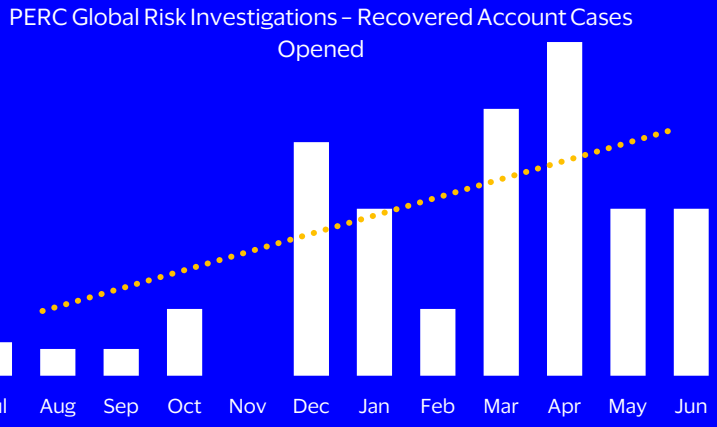
This public edition of Visa's Biannual Threats Report distills insights from Visa's global intelligence network into five defining forces reshaping payment security — and how Visa is working with partners across the ecosystem to address them.

Force 1: The Industrialization of Fraud
From Artisan to Assembly Line

The Pattern:
Fraud has evolved from opportunistic crime into systematic, industrial-scale operations. Criminals are building reusable infrastructure — botnets, synthetic identities, templated scam scripts, and AI tooling — that can be deployed across multiple attack types simultaneously, with the efficiency and scalability of a tech startup.

Evidence Across Threats:
Underground forums show a 477% increase in mentions of "AI Agent" as criminals discuss automating social engineering, data extraction, and transaction execution. Carding shops like BidenCash operate "Anti-Public Systems" that scan and remove duplicate data to ensure released datasets are exclusive and valuable, treating stolen credentials as managed inventory with quality control and vendor penalties for redundant records. Scam networks use standardized operational playbooks, rotating through job scams, romance scams, and investment schemes with industrial precision. The shift is visible in the data: Visa PERC tracked a 220% surge in Recovered Accounts cases over the past six months, driven by mass data dumps that flood criminal markets with hundreds of thousands of accounts in single releases. These data dumps are coordinated product launches designed to drive traffic, build marketplace reputation, and establish criminal brand equity before monetizing through premium sales or fraud-as-a-service offerings.





What It Means:
Fraud has evolved from reactive or opportunistic — it's moved to strategic, automated, and scalable. Criminals operate with R&D cycles, go-to-market strategies, and continuous improvement processes. This industrialization means defenses must also transform: moving from case-by-case fraud detection to intelligence-driven disruption of criminal infrastructure before it scales.

Visa's Response:
Visa's Scam Disruption (VSD) program uses AI-powered analytics and global intelligence sharing to identify and dismantle scam networks before they reach critical mass. By monitoring underground forums, analyzing transaction patterns across the network, and coordinating with financial institutions and law enforcement globally, Visa disrupts the infrastructure criminals depend on — shutting down fraudulent merchant accounts, blocking money movement channels, and sharing threat intelligence in real time to prevent copycat operations.

Force 2: The Monetization Playbook
Fraudsters Shift Speed and Strategy to Maximize Value

The Pattern:
Criminals don't just steal data — they strategically time and distribute it to maximize return on investment. They operate with dual-speed strategies: moving slowly and deliberately when stockpiling stolen credentials to maximize reach and evade detection, then shifting to maximum velocity when monetizing to outrun fraud controls.

Evidence Across Threats:
Detailed analysis of payment data recovered from BidenCash and B1ack's Stash revealed that 85-93% of exposed accounts were linked to enumeration attacks that occurred at least 12 months prior. Criminals are aging stolen credentials — letting accounts settle, victims move on, and monitoring fatigue set in — before releasing them strategically to underground markets.

When they do move to monetize, speed becomes the weapon. Scams increasingly exploit instant payment channels — real-time payments, digital wallets, cryptocurrency — to move stolen funds across borders in seconds, making recovery nearly impossible. In one documented case, a fraudulent employment agency collected fees through neobank platforms with weak security protocols, then disappeared before victims could react or financial institutions could intervene. Token provisioning fraud leverages the speed of mobile wallet onboarding: criminals use scripts to test thousands of card numbers through merchants' card-on-file systems, validating credentials in real time before conducting high-dollar transactions at fraudulent merchants established outside the card's issuing country.

What It Means:
The 12-month lag between compromise and exploitation creates a persistent, latent risk pool that traditional real-time fraud detection struggles to address. Consumers believe "if my card hasn't been used fraudulently yet, I'm safe" — but their data may already be in a criminal warehouse waiting for the optimal monetization moment. And when that moment comes, the money moves so fast that by the time fraud is detected, recovery is difficult, if not impossible.

Visa's Response:
Visa combats this through dual-speed defense:

Slow-phase: Visa's capabilities like Visa Payment Threat Intelligence (monitors dark web forums and carding shops), Visa Account Attack Intelligence (identifies accounts compromised through card testing), and the Breach Identification Tool (identifies account compromised through traditional data breaches) enable identify vulnerable accounts before they're monetized and alerting issuers to secure them proactively. This enables predictive mitigation rather than reactive response.

Fast-phase: Visa's real-time authorization systems, velocity controls, and AI-powered fraud models detect and block monetization attempts in milliseconds — whether through token provisioning, instant payments, or distributed enumeration. Visa Token Service provides step-up authentication for suspicious provisioning attempts, and Visa Advanced Authorization applies dynamic risk scoring to every transaction.

By operating at both speeds, Visa matches the adaptive monetization strategies criminals use to exploit the payments ecosystem.

Force 3: The Authenticity Crisis
AI Makes Everything Fakeable

The Pattern:
We're entering an era where nothing can be trusted at face value. AI enables the creation of synthetic content — fake merchant websites, fake identities, fake conversational agents, fake compliance documentation — that is indistinguishable from legitimate business materials. Traditional fraud signals that relied on visual inspection, documentation review, or conversational authenticity are becoming unreliable.

Evidence Across Threats:
Scam merchants successfully onboard using legitimate-looking merchant names and convincing merchant category types like Marketing/Consulting Services, Government Services, and Travel Agencies. These merchants pass basic compliance checks because their websites, business documentation, and operational facades are professionally constructed — often with AI assistance. Once onboarded, they process fraudulent transactions under the cover of legitimate business categories, making detection significantly harder.

The sophistication extends to social engineering. Modern scams use AI-powered conversational agents that adapt in real time, building trust through personalized, context-aware dialogue that traditional phishing emails could never achieve. Romance scams, investment schemes, and job offers are delivered through longer-duration engagements that feel authentic because they're dynamically generated to match victim psychology and behavior.

In the underground economy, criminals are actively experimenting with autonomous systems that can conduct reconnaissance, initiate contact, maintain conversations, and execute transactions — all without human intervention. The report notes that synthetic content is now "indistinguishable from legitimate business materials," meaning verification processes that worked for decades are suddenly less effective.

What It Means:
The authenticity crisis creates a trust vacuum. If AI can fake anything — websites, identities, conversations, documentation — how do consumers and institutions distinguish real from fake? Traditional due diligence (Does this look professional? Does this person sound legitimate? Are the documents in order?) no longer provides reliable signal. This isn't just about deepfake videos — it's about fake businesses, fake identities, and fake trust woven seamlessly into the payments ecosystem.

Visa's Response:
Visa is developing the Trusted Agent Protocol — a standards-based framework that moves beyond visual inspection to verify agent identity and intent through cryptographic attestation, behavioral analysis, and continuous telemetry. The protocol enforces verified identity fields, applies time-based transaction challenges that are difficult for AI to circumvent, and integrates real-time monitoring that detects operational changes indicative of AI-driven fraud.

For merchant monitoring, Visa goes beyond MCC and visual inspection to analyze transaction patterns, dispute rates, chargeback velocity, and cross-network behavior — signals that are harder to fake with synthetic content. Visa's **$12B** investment in fraud and security over the past five years includes advanced machine learning models trained to detect the subtle patterns that distinguish legitimate operations from sophisticated fakes, even when surface-level indicators appear authentic.

Force 4: The Control Erosion Problem
Legacy Defenses Are Becoming Unreliable

The Pattern:
Traditional fraud controls — velocity checks, merchant categorization, visual website inspection, delayed fraud monitoring, perimeter-based security — were designed for a world where fraud moved at human speed, fake businesses looked amateurish, stolen data was used immediately, and payment entities were the primary targets. None of those assumptions still hold, creating a control erosion problem where defenses that once provided a bulk of the effectiveness may now catch only part of threats.

Evidence Across Threats:
Enumeration attacks distribute testing across merchants globally, using low-velocity probing that stays under traditional rate-limiting thresholds. In a newly identified provisioning tactic, criminals abuse customer accounts at large eCommerce merchants and the process of adding an account to a wallet at the merchant. Threat actors look for signals that the account is valid— but because the testing is distributed and low-velocity at each individual merchant, traditional velocity controls often can't detect the coordinated attack.

Scam merchants, often have higher-than-typical decline rates — yet the merchants remain active because they use legitimate MCCs and pass basic compliance checks. The fraud is visible in transaction-level data, but invisible to merchant-level controls that rely on categorization and documentation review.

What It Means:
The defenses we've relied on are becoming obsolete faster than they can be replaced. Rule-based controls can't detect distributed attacks. Threshold-based systems miss low-and-slow tactics. Human review can't scale to AI-generated synthetic content. And perimeter defenses fail when the breach happens at a third party outside the perimeter.

This creates an arms race where defenders are in danger of falling behind — not because they're not investing, but because the pace of adversary innovation is outstripping the pace of control evolution.

Visa's Response:
Visa is replacing static rules with dynamic intelligence:

AI and machine learning models detect coordinated, distributed attacks invisible to traditional velocity controls by analyzing patterns across the entire network rather than at individual merchant or issuer level

Behavioral analytics identify anomalies in merchant operations, transaction flows, and account activity that signal fraud even when surface-level indicators appear normal

Proactive account protection through Visa Account Attack Intelligence (VAAI) identifies compromised credentials before they're monetized, rather than waiting for fraud to occur

Ecosystem hardening through programs like VARS (Visa Acceptance Risk Standards) extends security requirements beyond financial institutions to acquirers, processors, and service providers

The shift is from reactive blocking to proactive disruption, from perimeter defense to ecosystem resilience, and from rule-based detection to intelligence-driven prevention.

Force 5: The Third-Party Vulnerability Gap
The Weakest Link Is Outside the Financial Institution

The Pattern:
The most significant vulnerabilities and highest-impact breaches are occurring outside traditional financial institutions — at third-party service providers, processors, merchants, and non-financial ecosystem participants. As traditional institutions have hardened their defenses through PCI DSS compliance, advanced fraud detection, and regulatory pressure, criminals have shifted focus to the weakest links in the payments value chain.

Evidence Across Threats:
Visa PERC reported a 41% increase in ransomware incidents affecting payments ecosystem entities from January to June 2025 compared to the previous six months. The data reveals an overall upward trend with significant spikes in February 2025 and increased volatility, demonstrating a growing and more unpredictable ransomware threat landscape.

The analysis of Agent Cases from January to June 2025 showed a 173% increase in Compromised Account Management System (CAMS) account distribution compared to the same period in 2024. This reflected higher-volume incidents that significantly increased potential exposure. The period-over-period comparison reinforced this trend: case counts had remained stable or declined, while the total accounts distributed per case had increased. Visa continues to encourage agents to strengthen access controls, monitor for unusual activity, and follow Visa's *What to Do if Compromised* procedures — in alignment with PCI compliance requirements. These actions directly address the patterns seen in recent data, where a small number of high-volume cases accounted for the majority of CAMS account exposure.

These attacks highlight the vulnerabilities of third-party payment providers and underscore the importance of robust access controls, secure integration methods, and strict adherence to PCI DSS standards to protect against digital skimming and large-scale data breaches.

What It Means:
The payment ecosystem is only as strong as its weakest participant. A ransomware attack on a payment services provider can cascade into payment disruption. A compromised third-party payment gateway can expose millions of accounts. A poorly vetted merchant can become a scam platform. And because these entities operate across multiple payment networks and jurisdictions, a breach at one third party can impact the entire ecosystem.

This creates a trust paradox: consumers trust their bank's security, but their payment data is often exposed through a merchant, processor, or vendor they've never heard of and have no relationship with.

Visa's Response:
Visa is addressing the third-party vulnerability gap through ecosystem-wide defense:

Merchant monitoring and risk scoring continuously assess merchant behavior, dispute rates, and cross-network patterns beyond initial onboarding

Third-party risk management frameworks require acquirers to validate the security posture of their processors and service providers

PCI DSS enforcement and validation across all ecosystem participants that store, process, or transmit payment data

Layered security recommendations including multi-factor authentication (MFA), intrusion detection, file integrity monitoring, and restricted third-party integrations to harden the weakest links

Real-time intelligence sharing to alert ecosystem participants when third-party compromises are detected, enabling rapid containment

The shift is from institution-centric security to ecosystem-wide resilience, recognizing that payments are only as secure as the weakest participant in the value chain.

Closing Perspective: Building Resilient Commerce

The five forces reshaping payment security — industrialization, adaptive monetization, synthetic authenticity, control erosion, and third-party vulnerability — represent a fundamental transformation in how fraud operates. Criminals are faster, smarter, more coordinated, and more sophisticated than ever before. But so are the defenses.

Visa's role is clear: to anticipate, detect, and disrupt emerging threats before they can impact consumers and businesses. By combining global intelligence, advanced AI and machine learning, collaborative partnerships across the ecosystem, and a commitment to continuous innovation, Visa is helping ensure that the future of commerce is both innovative and inherently secure.

The payment threat landscape will continue to evolve — but no single organization can address these threats alone. The scale and cross-border nature of financial crime demand coordinated industry action. Visa is working with payment networks, banks, regulators, technology providers, and law enforcement to establish intelligence-sharing frameworks, early detection capabilities, and coordinated rapid-response strategies. This collaborative approach is essential to counter adversaries that can operate simultaneously across multiple jurisdictions and platforms. Visa's commitment to protecting every transaction, regardless of size or how you pay, remains constant. Working 24/7 across the globe, Visa is building the resilient commerce infrastructure the world depends on.

ACKNOWLEDGEMENTS

The authors would like to thank the numerous contributors across Visa PERC, Visa Risk Management Information Systems (MIS), Visa Risk Managed Services, and the entire Visa Risk organization.