White Paper

Fighting card enumeration fraud

Unlock broader defenses against a systemic global threat

Are you equipped to combat card enumeration fraud?

Card enumeration is one of the most persistent and least visible fraud threats facing the global payments ecosystem. Dismiss it all you like as low-value transaction noise, but enumeration has become a primary entry point for large-scale card-not-present fraud, downstream account compromise and operational disruption.

As digital commerce continues to expand and move more money than ever, fraud actors increasingly exploit gaps between merchants, acquirers, processors and issuers. And because enumeration attacks frequently occur below traditional fraud thresholds, they can easily stay undetected until losses materialize elsewhere in the ecosystem.

To fight back against this threat, you need to take a coordinated, intelligence-driven approach that moves beyond isolated controls and toward ecosystem-level risk management.

Know your enemy: The shape and size of card enumeration fraud

Card enumeration attacks automate the testing of payment credentials such as primary account numbers, expiration dates, verification values and postal codes through live authorization attempts.

The objective is not immediate fraud, but validation. Once valid credentials are confirmed, they can be monetized through fraudulent purchases, account takeover or resale in underground markets.

There are consequences for the entire payments ecosystem. Rather than targeting a single participant, enumeration exploits structural fragmentation across digital merchants and payment gateways, acquirers and payment facilitators, processors and networks, and issuers and fraud operations teams.

No wonder that Visa has consistently identified enumeration as a top ecosystem risk. With the ability to generate large volumes of fraudulent authorization attempts, automated card testing creates downstream losses well beyond the original point of attack.[1]

Operational impacts of enumeration across the payments ecosystem

Issuers face immediate fraud losses, card-reissuance costs and increased demand for customer service. When enumeration attacks are publicized, there can also be long-term erosion of cardholder trust and reputational damage.

Acquirers and processors risk increased authorization costs, compliance breaches and merchant remediation issues, particularly as network monitoring programs expand.

Merchants experience infrastructure strain, higher chargeback rates and potential monitoring or enforcement actions when their environments are exploited for enumeration activity.

These impacts are cumulative and often disconnected from the original point of attack, underscoring the systemic nature of the risk. [2]

[1] Visa, Biannual Threats Report, Spring 2025

The global impact

Global payment card fraud losses reached $33.41 billion in 2024,[3] with the majority of losses worldwide coming from card-not-present transactions. The U.S. alone accounted for more than 42% of global card fraud losses, despite generating only around one quarter of global card volume.[4]

Enumeration acts as a force multiplier within this environment. Visa estimates that enumeration attacks and related testing activity contribute to over $1 billion a year in follow-on fraud losses, driven by the reuse and resale of validated credentials across multiple channels.[5]

Industry intelligence shows that a meaningful share of accounts experience fraud within days of being exposed by enumeration. The majority see fraudulent activity within months, creating a delayed but material impact for issuers and merchants.[6]

The evolution of enumeration attacks

Over the past three decades, changes in payment technology and commerce models have seen enumeration techniques evolve considerably.

In the 1990s and early 2000s, early enumeration attacks relied on manual or semi-automated testing of card numbers across a limited set of merchants. As e-commerce expanded in the 2010s, attackers adopted scripts and bots to iterate bank identification number ranges using predictable card structures.

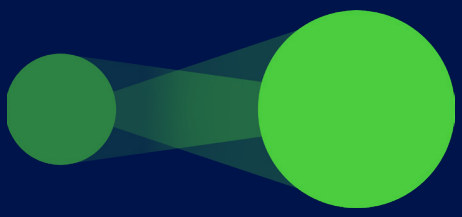
Since 2020, enumeration has become highly distributed. Attacks are now spread across thousands of merchants, IP addresses and devices to evade velocity-based detection. More recently, threat actors have begun exploiting recurring transactions, newly onboarded merchants and authentication flows to bypass traditional controls and blend into legitimate traffic patterns.[7]

How enumeration attacks work

A typical enumeration attack progresses through four stages.

1. Fraudsters generate potential credential combinations using known bank identification number ranges and algorithms.
2. Automated tools submit thousands of authorization attempts across multiple merchants while varying verification values, expiration dates, and postal codes.
3. Attackers analyze authorization and authentication responses to confirm valid combinations.
4. Validated credentials are monetized through fraud, sold on underground markets, or used in account takeover schemes.

Because the overwhelming majority of enumeration attempts are declined, the activity often appears benign until validated credentials are exploited elsewhere, making early detection critical.[8]



[2] Visa, Biannual Threats Report, Spring 2025
[3] Nilson Report, Card Fraud Losses Worldwide in 2024
[4] Fintech Futures, Payment Card Fraud Losses Approach $34 Billion,January 6, 2025
[5] CardRates, Compliance Deadline Nears for Enhanced Visa Fraud Program, September 11, 2025
[6] Visa, Biannual Threats Report, Spring 2025
[7] Visa, Biannual Threats Report, Spring 2025
[8] CardRates, Compliance Deadline Nears for Enhanced Visa Fraud Program,September 11, 2025

Current and future threats

Modern enumeration attacks tend to be highly automated, using botnets and device emulation. They also typically initiate low-value or zero-value transactions to minimize detection.

Specific merchant categories are particularly under threat, such as digital goods, food services, medical services, charitable organizations and subscription services. As well as commonly supporting low-value, frictionless and card-on-file transaction types, these frequent targets of fraudulent activity have historically had weak or uneven fraud controls.

Cross-border and cross-channel payments, including credential-on-file and recurring transactions, are also vulnerable. Cross-border activity can often help fraudsters evade geographic, risk-based controls and route enumeration attempts through foreign IPs and devices. Cross-border traffic is "noisier" and harder to pattern-match, making it a perfect breeding ground for enumeration, which succeeds when no single entity can see the full pattern.

However, Visa threat reporting shows that attackers increasingly shift targets based on which sectors or service providers demonstrate weaker controls at a given time.[9]

Why existing industry solutions fall short

With a growing requirement for continuous monitoring and adaptive defenses, the banking and payments industry urgently needs more effective solutions to combat enumeration fraud. Over the next three years, enumeration risk is only expected to intensify due to continued growth in digital commerce and wider use of automated attack tooling.

Despite heightened regulatory and network scrutiny, there is likely to be increased exploitation of newly onboarded merchants, and research indicates that threat actors will continue to combine enumeration with other techniques such as provisioning fraud, authentication bypass and social engineering.[10]

So, it's never been more important to detect enumeration attacks at the earliest opportunity and mount a coordinated defense. But the question is: how?

It's become clear that traditional fraud controls were not designed to address enumeration at scale. While merchant-level controls lack visibility into broader patterns at the bank identification number (BIN) level, issuer-centric detection only identifies fraud after accounts are compromised.

Static velocity rules can be easily bypassed by distributed, low-and-slow attacks. Siloed tools are unable to correlate activity across merchants, acquirers and networks. Traditional neural-network models focus on a cardholder's normal spending behavior, not the rapid, low-value, cross-BIN probing patterns that characterize enumeration attacks.

As a result of these limitations, enumeration activity can persist for extended periods before coordinated action is taken, increasing the vulnerability of the ecosystem-aware defense.[11]

Recommended solutions and their business value

To more effectively tackle enumeration fraud, participants in the payments ecosystem need to shift from reactive fraud management to proactive, ecosystem aware defense.

By detecting patterns across issuers, merchants and networks rather than isolated entities, you can get a more holistic picture of fraudulent activity. But time is also of the essence. Real-time anomaly identification across authorization attributes and transaction flows helps stop fraud in its tracks – and coordinated response mechanisms reduce time to containment.

You also need more flexible, dynamic fraud management operations. That means adaptive thresholds which evolve with emerging attack tactics, and operational support models which reduce internal burden while improving outcomes.

Ultimately, organizations with deep transaction visibility, advanced analytics and deep experience of operating at ecosystem scale are best placed to deliver these capabilities, while keeping money in motion with legitimate commerce.

[9] Visa, Biannual Threats Report, Spring 2025
[10] Visa, Biannual Threats Report, Spring 2025
[11] CardRates, Compliance Deadline Nears for Enhanced Visa Fraud Program, September 11, 2025

Unlock intelligence-driven defense

Card enumeration fraud is no longer a background technical issue. It's a foundational threat vector that enables downstream fraud at scale and significantly increases costs across the payments ecosystem. Addressing it requires collaboration, intelligence and technology that operates beyond individual silos.

Organizations that invest in holistic, intelligence-driven enumeration defense will be in a stronger position to reduce losses, protect customers and support sustainable growth in an increasingly digital payments environment. Are you ready to reinforce your defense strategy?

Fight card enumeration fraud with the power of FIS®. Our advanced fraud management capabilities and solutions can help you address this pervasive industry threat.

Unlock more

Money at rest. Money in motion. Money at work.™

Our technology powers the global economy across the money lifecycle.

Money at rest

Unlock seamless integration and human-centric digital experiences while ensuring efficiency, stability, and compliance as your business grows.

Money in motion

Unlock liquidity and flow of funds by synchronizing transactions, payment systems, and financial networks without compromising speed or security.

Money at work

Unlock a cohesive financial ecosystem and insights for strategic decisions to expand operations while optimizing performance.

fisglobal.com/contact-us linkedin.com/company/fis x.com/fisglobal

FIS | Advancing the way the world pays, banks and invests™