FraudNet

ENUMERATION ATTACK DETECTION

Card Testing Moves in Hours. Most Fraud Stacks Still Think in Days.

How enumeration attacks actually work, why the old playbook is falling behind, and what's catching them in real time.

The Threat Is Mainstream, and Accelerating

33%

of merchants report card testing among their top five fraud types.

Visa 2025 Global eCommerce Payments & Fraud Report

+7,851%

year-over-year growth in AI-agent traffic.

HUMAN Security, 2026 State of AI Traffic & Cyberthreat Benchmark Report

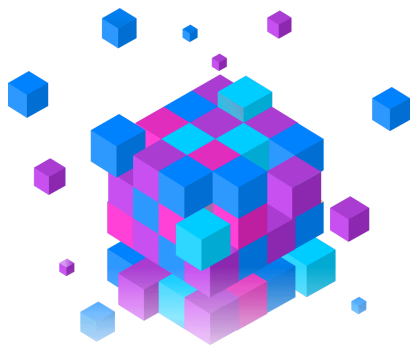
WHAT IS CARD TESTING?

Running large volumes of small authorization attempts against stolen or guessed card numbers, searching for the ones still live. Each attempt costs almost nothing to run — but for the merchant on the other end, every attempt still touches the payment stack: an authorization request, a risk decision, sometimes a hold on inventory.

HUMAN Security's 2026 State of AI Traffic & Cyberthreat Benchmark Report found AI-agent traffic climbing 7,851% year over year — nearly 80-fold growth in the volume of bots and agents operating across the web. More agents in circulation means more card-number combinations tested, faster, compressing what used to be a slow, exploratory process into something that can run its course in minutes.

WHY THE NUMBERS KEEP CLIMBING

- Card testing already ranks among merchants' top five fraud types, alongside real-time payment fraud, phishing, and first-party misuse.
- AI-agent traffic is climbing nearly 80-fold year over year.
- Each attempt is cheaper to run and harder to distinguish from legitimate automated tools than a few years ago.

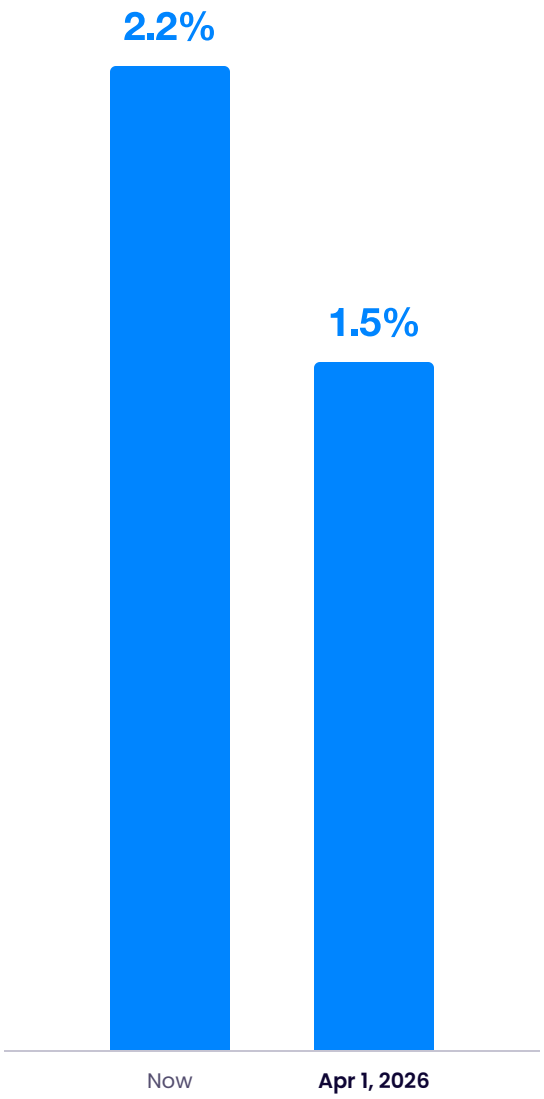


Now a Compliance Problem, Too

Chargebacks are a lagging indicator. Under VAMP, they're also an expensive one.

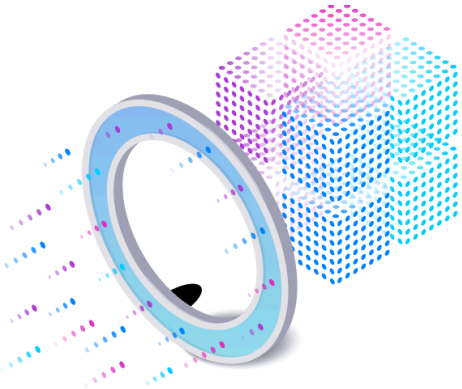
There's no warning tier. Merchants are either under the threshold, or they're in "Excessive."

COMBINED FRAUD + DISPUTE CEILING



HOW VAMP CLASSIFIES "EXCESSIVE"

- Dispute ratio ceiling dropped to 1.5% of settled transactions (from 2.2% today), effective April 1, 2026.
- **Enumeration Ratio:** more than 20% of a merchant's monthly authorization attempts flagged as card testing, at ≥300,000 attempts that month, means automatic "Excessive," regardless of dispute ratio.
- Applies only once a merchant clears 1,500 combined fraud reports + disputes a month, so smaller merchants have room to breathe.
- Above that line, card testing stops being an operational headache and becomes a compliance exposure with a number attached.



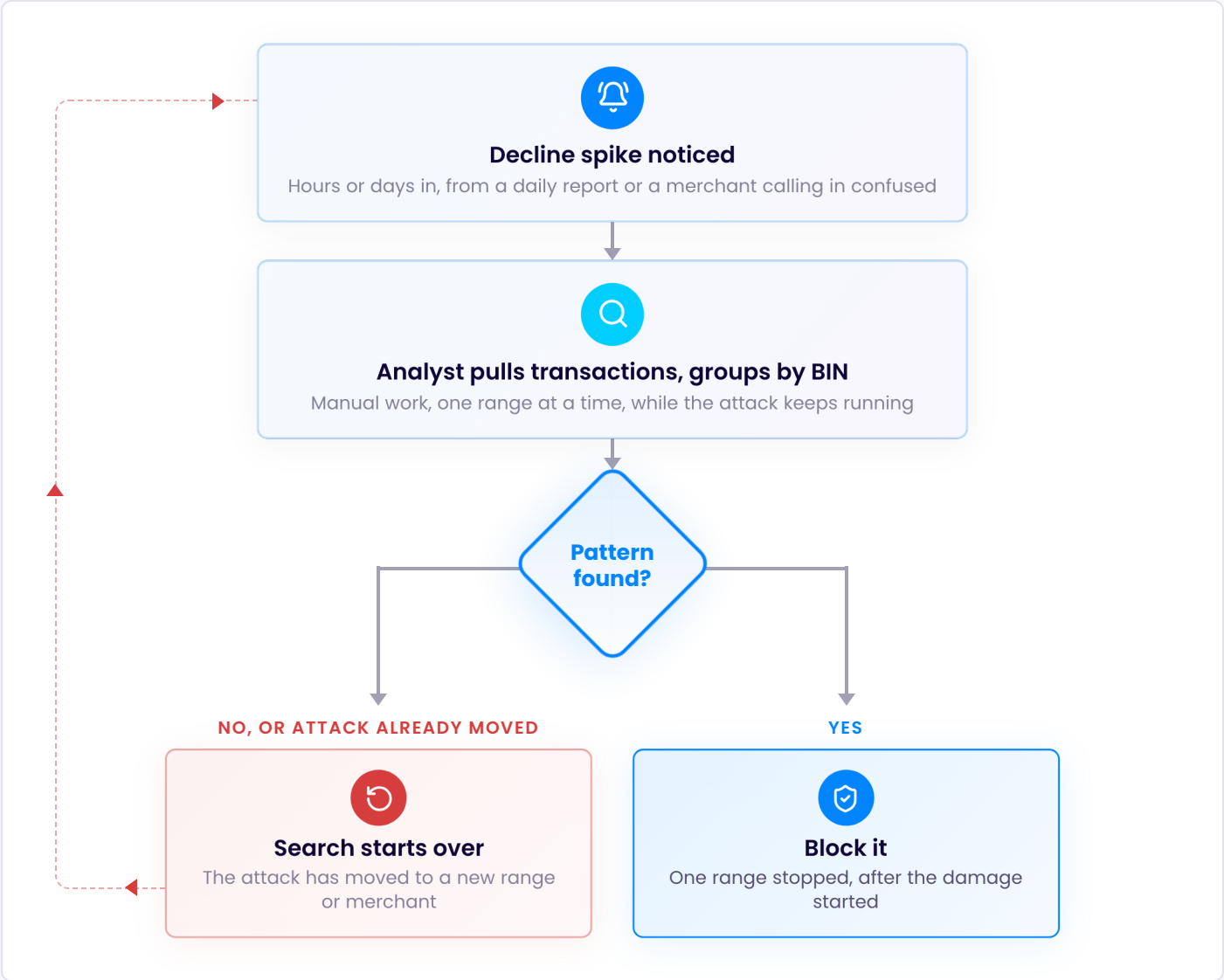
20%
Enumeration Ratio

≥300,000
monthly attempts

1,500/month
TC40+TC15 minimum

The Manual Playbook

Picture how most fraud teams still catch this. A spike in declines gets noticed, maybe in a daily report, maybe because a merchant calls in confused about a wave of failed charges. An analyst pulls the transactions, groups them by BIN, and starts looking for a pattern by hand. Find one, and they can block it. Miss it, or catch it after the attack has already moved to a different card range or a different merchant on the same platform, and the search starts over.



It works, but only after someone notices, and only for the range someone happens to be looking at.

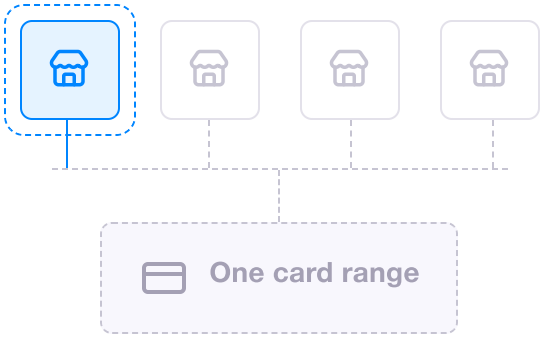
With the manual approach, your analysts are always a step behind - while card testing is becoming faster, easier, and more automated.

Same Attack. Two Ways to Catch It.

Traditional velocity rules watch a single merchant's transaction volume and flag when it looks abnormal for that merchant. That catches a bad actor hammering one storefront, but modern card testing rarely stays in one place. The same batch of stolen numbers gets tested across dozens of merchants on the same platform, in small enough volumes at each one that no single merchant's velocity rule ever fires.

Range-level detection looks at the card numbers themselves, not just where they're being used. When authorization attempts against the same block of numbers show up across multiple merchants, that pattern is visible at the range level even when it stays invisible at the merchant level.

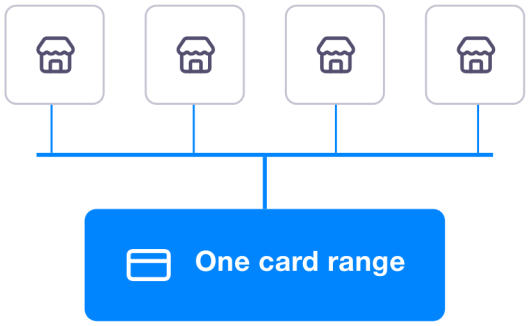
OLD WAY



Merchant-level rules catch the merchant.

Each merchant is watched on its own. Testing spread thinly across the other three never trips a threshold, so the shared card range goes unseen.

NEW WAY



Range-level signals catch the pattern.

Attempts against the same card range are correlated across every merchant at once, so the attack surfaces even when no single merchant looks unusual.

Automate the manual work. Give your best analyst their time back.

CASE STUDY

Card Testing, Caught in Real Time

Card testing detection runs inside FraudNet's Merchant Risk Monitoring platform. Applied directly to client data, it surfaced card testing activity that existing manual processes had missed or mischaracterized.

THE PROBLEM

- Manual investigations forced to hunt patterns by hand.
- Signals and exports arrive too late to act on.
- Card testing slipping through until it surfaced as a chargeback.

THE APPROACH

FraudNet's Merchant Risk Monitoring platform, with card testing detection enabled: continuous, real-time monitoring of card prefixes for anomalous patterns across every merchant on the portfolio.

THE RESULTS

NATIONAL MERCHANT ACQUIRER

24 hrs

from activation to first catch

Card testing surfaced on the first day the platform was live. 65 transactions flagged on a single merchant, same amount, same prefix, all declined before chargebacks hit.

ANONYMIZED PAYMENTS CLIENT

16,772

transactions in 17 hours

One card range generated 16,772 transactions in 17 hours across 48 prefixes. Every one declined. Caught in real time, before a single chargeback posted.

These aren't isolated incidents. Over six months of continuous monitoring across one of FraudNet's clients, a major merchant services provider in the United States, the same pattern holds:

55.9M	943	136K
transactions monitored	attack prefixes surfaced	attack transactions flagged

6 months, live production

Always-On, Not Ad Hoc

The gap between catching an attack and missing one usually comes down to timing, whether monitoring is already running or waiting for someone to notice first. FraudNet's Merchant Risk Monitoring platform runs the continuous side.

Manual review

- ✕ Waits for someone to notice
- ✕ Checks one range at a time
- ✕ Catches an attack after a threshold trips

Continuous monitoring

- ✓ No trigger needed
- ✓ Watches every range, all the time
- ✓ Catches an attack while it's still running

From Signal to Action

Detection only matters if it leads somewhere. Here's what happens between a card range crossing a threshold and an analyst actually stopping it.

1. **Monitor** — every range, continuously
2. **Flag** — behavior crosses a tunable threshold
3. **Alert Fraud Ops** — with enough context to act
4. **Act** — before it's a chargeback, before it moves elsewhere

Card testing isn't slowing down, and under VAMP, finding out about it late now comes with a price tag.

See how this holds up against your own card ranges.

Request a Demo