



SPONSORED

# Payments in the age of VAMP

Published July 21, 2025

BY [unreadable] [unreadable] [unreadable] [unreadable] [unreadable]



Shutterstock / Smile Studio AP

SPONSORED CONTENT BY 

It may sound like shorthand for Dracula’s job title, but VAMP is actually a new set of security measures and requirements coming to the world of payments. Add another acronym to your buzz list, here comes the “Visa Acquirer Monitoring Program.”

## Why are we VAMPing?

The payment ecosystem is evolving: More consumers, more merchants, bigger enterprise players, millennial leaps in the ways people pay — it all comes with elevated fraud, disputes, and enumeration challenges.

Enumeration — or “card testing” — is a rapid, brute-force attack in which fraudsters bulk test stolen card data for validity; it leads to annual losses in the billions. Disputes are another concern. They occur when consumers call purchases into question — “I didn’t buy this! I’m not paying for it!” According to the [Wall Street Journal](#), they resulted in \$11 billion worth of charges with U.S. card issuers in 2023 alone.

The risks in ecommerce are rising. The challenges are becoming more sophisticated, automated, and pervasive. Enter VAMP.

The new program aims to streamline how Visa tracks and addresses fraud, disputes, and chargebacks in payments — notably where they occur in online, card-not-present transactions. Existing security measures helped Visa prevent over \$40 billion in fraud in 2023. That staggering number, however, hints at a monster lurking in the shadows — and the need for payment processing to up its game. With VAMP, Visa [says](#) it “seeks to ultimately reduce fraud and enumeration across the global payments ecosystem by helping acquirers improve their risk controls.”

Visa is setting out to create seamless controls and processes that they claim will tackle four times the amount of global fraud, significantly reduce loss, and make the ecommerce world a safer place for everyone.

### **How VAMP works**

The new program is built on the twin pillars of the [Visa Dispute Monitoring Program](#) and the [Visa Fraud Monitoring Program](#), creating a new, singular pillar with some significant new processes, rules, and requirements entering the mix. The program uses a formula to determine a “VAMP ratio,” which is calculated by dividing the sum of fraud and dispute transaction counts by the

number of settled transactions. This ratio becomes the core metric for Visa's monitoring compliance.

The VAMP ratio includes both fraud reports (TC40) and all disputes (TC15), which means fraud-related disputes are actually counted twice. So if a TC40 report leads to a chargeback, it will impact your VAMP ratio even more.

### **Know your limits**

VAMP ratios determine thresholds for merchants and acquirers. If they exceed their limits, these players become identified as “high-risk,” a label that, in Visa's world, comes with penalties in the form of fines and heightened monitoring.

Starting April 1, 2026, that means an acquirer VAMP ratio of 0.7% and a merchant ratio of 1.5% are considered “excessive” — and they may get hit with higher fees and penalties.

Riskified has a more in-depth look at essential VAMP information on their [site](#).

### **The merchant's burden**

While VAMP brings new levels of security and protection, it also comes with significant stressors for merchants. In this new era, they may be looking at:

- **Increased scrutiny** from Visa and their acquirers if they exceed VAMP thresholds.
- **Penalties** for failing to comply with new rules — and staying within acceptable ratios.
- **Stronger prevention measures** to help them mitigate fraud, settle disputes, and stay within required thresholds.

## **Prepare to VAMP**

While this may sound like cause for concern, inspire sweaty palms, and stoke sleepless nights, there are payment processors anticipating VAMP's arrival. My company, Inovio by North, is one of them. We have in place a diverse set of security options to help shoulder a merchant's compliance burden — and prepare them for the stricter requirements of VAMP.

Here's 3 good reasons why Inovio is ready for VAMP:

### **1. We see VAMP in 3D**

"3-D Secure," that is. This is a security protocol already used by Inovio and legally mandated in Europe. It's designed to bolster existing security measures, adding an extra layer of protection for online credit and debit card transactions. By verifying the cardholder's identity with their bank during the checkout process, (think passwords, codes, multi-factor authentication and biometric verifications), 3-D Secure can significantly reduce fraud and chargebacks while providing more confidence for both merchants and cardholders in online transactions.

### **2. The speed of security**

Inovio brings customizable velocity settings to the security mix. This is an essential tool when combatting card testing. Our gateway enables you to set the amount of times a source can try card information — effectively hobbling the enumeration game played by so many fraudsters. As this is a key focal point for VAMP, having this tool in your security chest can make an enormous difference.

### **3. Route with wisdom**

Intelligent gateway routing and cascading are powerful tools for elevating your authorization rates. Inovio brings this resource to help you direct transactions to the MIDs that matter, cascading

failed payments to additional banks within our ecosystem to keep payments going. Higher auth rates mean less chargebacks, and overall transaction success keeps you in VAMP's good graces.

### **Don't fear the VAMP**

These new security requirements may mean a bit of work, but the results will be a more secure, safer ecommerce world. Finding the right payments partner can alleviate concerns, help you carry the requirements weight, and, ultimately, make better-informed business decisions.

Are you prepared for processing in the age of VAMP? Inovio is ready — and we have solutions to fit your business needs. Visit [us](#) to learn more