FraudNet

WHITEPAPER:

Changes to Dispute Thresholds:

What Should Merchants & Acquirers Do About Visa's New VAMP?

October 2025 Update

Contents

What Changed? Visa's VAMP Consolidation Explained

In May 2024, Visa announced a significant overhaul of its monitoring programs, leading to the rollout of the Visa Acquirer Monitoring Program (VAMP) in 2025. This new initiative consolidates the previous Visa Dispute Monitoring Program (VDMP) and Visa Fraud Monitoring Program (VFMP), with both programs being retired by March 31, 2025. **Starting April 1, 2025**, the unified VAMP program monitors fraud and dispute levels for all acquirers and their merchants, with enforcement set to begin on **October 1, 2025**. This guide has been created to help global e-commerce merchants and payment processors understand what's new and how to adapt.

Key elements of the change include:

01. Unified fraud & dispute monitoring

Visa has unified its fraud and dispute monitoring efforts by combining the Visa Dispute Monitoring Program (VDMP), Visa Fraud Monitoring Program (VFMP), and the legacy acquirer-focused VAMP into a comprehensive global framework[1,2]. This enhanced VAMP system introduces a single metric, the VAMP ratio, which measures all fraud reports and disputes relative to total transactions, replacing separate fraud and chargeback ratios[17,18].

Additionally, it streamlines 38 distinct remediation processes into a single cohesive program, simplifying compliance and establishing globally aligned thresholds for both domestic and cross-border card-not-present (CNP) transactions, providing greater clarity and consistency. However, some markets, such as Brazil, Chile, and India, will have a later rollout[19,20,21].

02. Risk-based, flexible enforcement (vs. automatic fines)

Visa has transitioned to a risk-based enforcement approach for its VAMP program, moving away from automatic fines for non-compliance[11]. Instead of imposing immediate penalties, Visa will charge fees only to those exceeding defined thresholds, such as "Excessive" merchants or "Above Standard" acquirers, with first-time offenders receiving a brief grace period (e.g., 3 months) before fees take effect[12].

This shift allows for greater flexibility, recognizes clients' varying risk appetites, and aims to focus on genuinely excessive outliers with graduated enforcement measures[26]. By structuring fees per dispute rather than imposing large immediate fines, Visa encourages collaboration on fraud reduction rather than simple punitive measures.

03. New thresholds & metrics

Under the VAMP framework, merchants and acquirers are subject to new, stricter dispute-rate thresholds, with merchants deemed "Excessive" if their VAMP dispute ratio exceeds 2.2% starting mid-2025, tightening to 1.5% for most major regions on April 1, 2026[3,4]. Acquirers face an "Excessive" threshold of 0.7% and an "Above Standard" warning tier at 0.5%.[5] Additionally, VAMP introduces a card-testing metric, where if over 20% of a merchant's transactions are flagged as card-testing attempts (with at least 300,000 such attempts), program action will be triggered.[6]

For Merchants:			For Acquirers:	
Now	April 1, 2026	Enumeration*	Excessive	Above Standard
2.2%	1.5%	20%	0.7%	0.5%

* Merchant's transactions identified as card-testing attempts

04. Advisory period and phased rollout

The updated VAMP program launched in Europe on April 1, 2025, with a phased rollout designed to support merchants and acquirers during the transition.[8] An advisory period ran from April to September 2025, allowing businesses to adapt without penalties.[8] Starting October 1, 2025, enforcement began for merchants and acquirers exceeding the "Excessive" thresholds, while enforcement for the "Above Standard" tier for acquirers will commence on January 1, 2026.[9,10] This timeline provides a transitional grace period that extends until the end of 2025, enabling businesses to adjust to the new, stricter rules effectively.[27]

1. **Updated VAMP takes effect in Visa Europe region** — **April 1, 2025**
2. **Advisory Period (no fines)** — **April–Sep 2025**
3. **Enforcement begins for Excessive thresholds** — **October 1, 2025**
4. **Grace period ends, Above standard enforcement begins (acquirers)** — **January 1, 2026**

05. Focus on fraud prevention and card testing

The updated VAMP program aims to strengthen fraud prevention by incentivizing stronger controls. By merging fraud and dispute metrics into a single ratio, even "friendly fraud" chargebacks are counted twice, increasing the risk for merchants with high illegitimate dispute rates.[14,6] Additionally, the inclusion of the enumeration metric highlights Visa's focus on combating card-testing attacks, requiring merchants to proactively detect and block these lower-value fraudulent attempts to safeguard cardholders and the network.[25]

Furthermore, the new program eliminates the "Above Standard" warning tier for merchants, meaning they will not receive advance notifications before facing penalties; they will either be below the threshold or classified as "Excessive." In contrast, acquirers still retain a two-tier structure, allowing for some flexibility[25]. As a result, merchants and acquirers must monitor their ratios proactively to avoid non-compliance penalties.

In summary, Visa's VAMP overhaul simplifies monitoring but raises the bar for acceptable fraud and dispute levels. It places **greater responsibility on acquirers** to police their merchant portfolios, and on merchants to keep their dispute metrics in check or face swift consequences. Next, we'll break down what these changes specifically mean for merchants and for acquirers.

VAMP Changes for Merchants: 4 Things You Need to Know

The new VAMP program introduces several significant changes for merchants regarding dispute thresholds and compliance requirements.

Here are four key changes that merchants should be aware of:

01. Unified Dispute-Fraud Ratio

Merchants will now track a single metric called the VAMP ratio, which combines the former separate "chargeback rate" and "fraud rate."

This ratio is calculated by adding total fraud reports (TC40) and total disputes (TC15) then dividing the sum by total sales transactions.[3] The denominator is the total number of settled Visa CNP transactions.

It encompasses all card-not-present disputes, including both "fraud disputes" (issuer fraud reports and fraud chargebacks, Visa reason code 10) and "non-fraud disputes" (chargebacks for authorization errors, processing errors, customer disputes — reason codes 11, 12, and 13).[4] It's important to note that this ratio counts incidents, not amounts — every dispute is treated equally, regardless of its dollar value.[22]

THE VAMP RATIO

This VAMP ratio is calculated as:

Total fraud reports **TC40** + Total disputes **TC15** ÷ **Total sales transactions**

02. Thresholds for Dispute Ratios

Visa has established an excessive dispute ratio threshold for merchants at 2.2% (220 basis points) initially in most regions[3]. Starting **April 1, 2026**, this threshold will be reduced to 1.5% for merchants in regions such as North America, Europe, and Asia-Pacific.[3,4] Merchants in Latin America and the Caribbean have already been held to a 1.5% threshold since the program's launch in 2025 and will continue to be held to this standard. If a merchant's monthly VAMP ratio exceeds the threshold while meeting the minimum dispute count (explained in point #3), they will be categorized as an "Excessive VAMP Merchant" and face additional oversight and fees. This change effectively lowers the tolerance for disputes, as many merchants who previously operated with a chargeback rate of approximately 0.9% will now need to keep their ratio under 1.5% after 2026[28].

03. Impact of Disputes on Ratios

Nearly every dispute will now have a greater impact on the ratio than before. A single fraudulent transaction can lead to both a fraud report and a chargeback, contributing to the ratio in two ways.[13] While Visa has stated that identical records will not be double-counted within the same month, a fraud incident often results in both a TC40 report and a chargeback over time, particularly in cases of "friendly fraud," where legitimate transactions are fraudulently disputed. Visa data indicates that **friendly fraud accounts for about 75% of all disputes**, meaning many chargebacks are accompanied by a fraud claim.[29] Under the VAMP program, all these disputes will factor into the unified ratio, emphasizing the necessity for merchants to maintain a low overall dispute volume, including fraud claims, to avoid exceeding the 2.2% or 1.5% thresholds.

04. New Enumeration (Card Testing) Ratio

VAMP introduces a second critical metric known as the **enumeration ratio**, which addresses card testing attacks — instances where fraudsters make numerous small authorization attempts to verify stolen card numbers. Previous programs did not thoroughly cover this type of fraud because it typically does not result in immediate chargebacks; however, Visa is now focusing on it. The enumeration ratio is the number of identified card-testing authorization attempts divided by the total number of authorization attempts (both approved and declined).[6]

Suppose more than 20% (2,000 basis points) of a merchant's authorizations in a month are flagged as enumeration attempts, and the merchant has at least 300,000 total attempts that month. In that case, they will be classified as "Excessive" under VAMP, even if their dispute ratio is low. This threshold applies globally and seeks to identify merchants being exploited by fraudsters for large-scale card tests.

The introduction of the enumeration ratio underscores that attempted fraud, not just successful chargebacks, can jeopardize a merchant's standing with Visa. Merchants who inadvertently permit large volumes of card testing, such as e-commerce sites lacking sufficient bot protection, may face increased scrutiny. **Visa's tool, Visa Account Attack Intelligence (VAAI)**, will help identify these enumeration patterns while minimizing false positives.[30] Most legitimate merchants with modern fraud-prevention measures already detect and mitigate such attacks, but this new rule places additional pressure on those that do not.

05. Exclusions for Resolved Disputes

A positive aspect of the VAMP program is that Visa will exclude certain disputes from the VAMP ratio calculation. Disputes that are resolved before they escalate into chargebacks through approved "pre-dispute" resolution channels (such as Rapid Dispute Resolution or partnerships with Verifi/Ethoca) will not count against a merchant's ratio.[31] This adjustment provides some relief for merchants by recognizing the effectiveness of preemptive resolution efforts.[32]

Understanding the recent updates to Visa's dispute resolution processes is vital for merchants and can really empower their business strategies. Initially, Visa communicated that disputes resolved through their Verifi tools, such as RDR and CDRN, would not impact VAMP calculations.[33] However, in March 2025, they made an important update: **fraud disputes characterized by a TC40 will indeed count against merchants, even if resolved via RDR.** This change is crucial for all merchants to consider as they navigate potential impacts on their operations.

As we look toward 2026, it's encouraging to note that non-fraud disputes that are resolved through pre-dispute solutions will be excluded from VAMP calculations. This means that if a customer dispute is resolved through credit, it won't influence the chargeback ratio, but keep in mind that fraud-related alerts (TC40) may still apply unless the CE 3.0 standard is in effect.[31,33] By viewing these exclusions as a silver lining, merchants can leverage tools like RDR as an invaluable safety net.

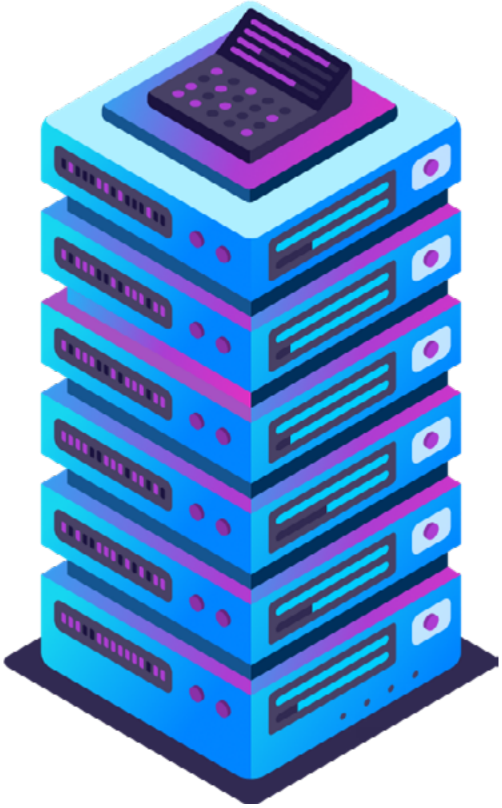
Another important takeaway is the removal of the "above standard" warning tier**. Merchants who exceed the VAMP threshold of 2.2% (or the upcoming 1.5%) will automatically enter the program without a grace period.**[25] While acquirers may provide informal warnings, formal notifications from Visa will not be forthcoming.

It's essential for merchants to consistently monitor their dispute levels, as there is no leeway to exceed the limit. Being out of compliance can have serious implications. To further safeguard their interests, acquirers may impose their own internal caps, so keeping well below these thresholds is sound advice.[34]

Lastly, remember that only Visa card-not-present (CNP) transactions processed through VisaNet are counted for VAMP.[35] In-person fraud and disputes are not included. There is a **minimum threshold of 1,500 combined fraud and dispute instances per month** for VAMP enforcement, meaning smaller businesses with fewer transactions can focus on managing disputes without fear of penalties.[40] This proactive approach is essential for profitability and nurturing strong partnerships with acquirers.

What About Acquirers? New Responsibilities and Thresholds

Monitoring Portfolio VAMP Ratio:



Visa is now tracking each acquirer's VAMP ratio across all merchants to improve the payments experience. This ratio is found by dividing the total number of fraud cases and disputes by the number of Card Not Present (CNP) transactions, evaluated at the portfolio level. An acquirer is "Above Standard" if their portfolio VAMP ratio is 0.50% or higher and "Excessive" if it reaches 0.70% or more.[41,42] Starting in late 2025, these thresholds will take effect.

By **January 1, 2026, the "Above Standard" range will change to between 0.30% and 0.50%**, while the "Excessive" threshold will stay at 0.70%.[43] This change is important—by 2026, acquirers with a ratio above 0.50% will be monitored more closely, and a ratio of 0.30%[43] could lead to helpful guidance. These new lower thresholds encourage acquirers to keep cleaner portfolios and show Visa's commitment to secure transactions.

Fees for Disputes

Visa will charge additional fees for disputes in an acquirer's portfolio if they are flagged. An acquirer labeled as "Above Standard" will pay $4 per dispute, while one considered "Excessive" will pay $8 per dispute.[13] These fees can add up quickly, especially for larger processors, motivating acquirers to stay compliant and reduce disputes. Visa offers a three-month grace period for the first time a problem is identified,[14] helping acquirers address concerns without immediately facing fees. However, if issues persist, acquirers may face financial penalties, potentially affecting non-compliant merchants. In serious cases, Visa may ask acquirers to reconsider their relationships with high-risk merchants.[45,46]

A key feature of this program is that it encourages acquirers to closely monitor their merchant portfolios. Visa expects acquirers to identify and address high-risk merchants—those with many disputes or frequent fraud issues—before they exceed the established thresholds.[47,48,49]

Focusing on High-Risk Merchants

The rules state that “Excessive” designations will only apply to an acquirer if their overall ratio exceeds the acquirer threshold. This ensures that acquirers with clean portfolios are not unfairly penalized for isolated issues. If an acquirer’s portfolio exceeds the 0.7% threshold, Visa will work with them to address the concerns instead of penalizing each merchant individually. This system encourages acquirers to promote compliance among their merchants since a few high-dispute merchants could negatively affect the entire portfolio. As a result, many acquirers are expected to set stricter internal standards, with some considering a 1% cap on their merchants’ VAMP ratios to keep the overall portfolio well below 0.5%.[34] Merchants might see stricter contracts or even offboarding if their fraud rates remain high, as acquirers are incentivized to manage risk responsibly.[50,51]

Global Rollout

VAMP will start in Europe, where many acquirers already follow strict regulations like PSD2, which promote low fraud rates and solid authentication. Since these acquirers monitor fraud rates closely for compliance, Visa will use this phase to collect valuable data and feedback. The program will then expand to other regions gradually; by late 2025, acquirers in the U.S., Canada, and Asia-Pacific are expected to adopt the same threshold structures, with enforcement likely following a similar global timeline (October 2025 for Excessive-level concerns, January 2026 for broader application).[18,52] This rollout encourages acquirers, especially in higher-risk sectors like gaming, gambling, travel, and subscription services, to be proactive and prepare for positive changes as Visa expands enforcement worldwide.

In summary, acquirers are expected to improve fraud and dispute oversight, invest in better risk tools, and collaborate with merchants to prevent issues. Michael Jabbara from Visa noted that acquirers in the Visa Advanced Merchant Program (VAMP) have about 10% fewer approved transactions compared to non-participants, indicating lost sales.

This means that **reducing fraud is necessary to boost approval rates and revenue.**[15,16] The new rules position acquirers as primary enforcers of Visa’s fraud standards, applying pressure through fees and the risk of losing merchant agreements if they do not comply.

How Can Merchants Be Proactive?

Merchants don't have to sit idle and wait to be flagged – now is the time to take action.

Here's a checklist of actions for merchants to prepare for VAMP and stay in compliance:

01. Know your numbers.

Start by calculating your current fraud and chargeback rates under the new formula. Look at your recent months of Visa transactions and figure out what your VAMP ratio would be (combine all fraud reports and disputes, divide by total Visa sales count). This will tell you if you're comfortably below the threshold or uncomfortably close.

Don't forget to include all disputes, not just fraud chargebacks – for many merchants, adding non-fraud chargebacks (like customer disputes) will bump the ratio up. **If you're near the ~2.2% mark (or 1.5% for LAC), take that as a warning sign.**

Also, consider your trajectory: are fraud and disputes trending up? Could a sudden fraud attack or a spike in friendly fraud push you over the line? It's crucial to anticipate scenarios like a surge during holiday season or a new marketing campaign that brings in higher risk orders. If your metrics are borderline, plan accordingly – you have to lower fraud incidence or increase sales volume (organically) to keep the percentage down.

02. Tighten fraud controls (within reason).

VAMP is fundamentally about encouraging better fraud prevention, so evaluate your current fraud screening and blocking rules.

If your fraud losses or dispute rates have been higher than they should be, it likely means your filters are too lax – you're letting too many bad transactions through. Consider raising your fraud rejection thresholds or adding new fraud rules to better block suspicious orders before they are approved.

Many merchants will need to shift their risk appetite to be more conservative now. However, beware of overcorrecting: you don't want to decline good customers en masse in a panic to cut fraud, which could hurt revenue.

The key is to use smarter fraud detection (machine learning models, consortium data, etc.) to block the right fraudsters rather than blanket declines. Aim to find that sweet spot where you're stopping the majority of fraud attempts (and thus avoiding both TC40 reports and chargebacks) while letting legitimate customers through with minimal friction. In short, if your fraud prevention solution isn't catching much, dial it up – but do so intelligently.

03. Review your chargeback management and alert systems.

Beyond preventing fraud, look at how you handle disputes when they do happen.

Do you use any chargeback alerts or deflection services (such as Ethoca alerts, Visa Order Insight/Verifi, Rapid Dispute Resolution)? If not, now is a great time to consider them.

These services can notify you of pending cardholder disputes or fraud claims before they turn into chargebacks, giving you a chance to refund or resolve the issue pre-emptively. Under VAMP, resolving a dispute at the pre-chargeback stage can keep it out of your ratio (especially for non-fraud disputes).[31]

Similarly, Visa's Compelling Evidence 3.0 initiative for fraud chargebacks might help you prevent or win back fraud disputes by providing better proof in cases of friendly fraud. Adopting these tools won't solve underlying fraud problems, but they can shave off dispute volume that would otherwise count against you.[55]

Essentially, **if you have ways to turn disputes into resolutions (refunds, etc.) before they hit the network as chargebacks, use them**. It could make the difference between 1.4% and 1.6% on your ratio, for example. And if you're already using such tools, ensure you're following best practices (e.g. responding quickly to alerts, fully leveraging the window to provide Order Insight data, etc.).

04. Talk to your acquirer.

Open a dialogue with your acquirer or payment processor about VAMP. Ask them how they are handling the new program and what they expect from you.

Some questions to consider:

- Will they pass through any VAMP fees to merchants (many will, as a clause in your merchant agreement – check the fine print if there's a "compliance fees" section)?
- Are they setting stricter internal thresholds for merchants to keep their portfolio clean?
- What happens if you do go above 2.2% – will they notify you, fine you, or even freeze funds?

Proactively understanding your acquirer's stance can help you avoid nasty surprises. If their answers aren't reassuring (say, they have no plan or they indicate your current dispute rate is a problem), you might even consider shopping around for a different acquirer with a more collaborative approach.

Keep in mind, though, that by 2026 all acquirers globally will be under this same pressure, so it's in your interest to get ahead of the issue rather than trying to hide from it. The merchant–acquirer relationship is becoming one of shared risk: make sure yours is a partnership, not an adversarial dynamic.

05. Ensure data transparency.

One practical step: make sure you are receiving all your chargeback and fraud data from the acquirer.

In some cases (especially if you have chargeback alerts or if liability shifts due to 3-D Secure), the acquirer might not forward certain fraud reports or chargeback notifications to you, because they assume it's "their problem." Insist on getting full visibility into every dispute that comes in related to your transactions.[47]

You can't fix what you can't see. For example, if issuers are filing fraud reports (TC40s) on transactions where 3-D Secure shifted liability to the acquirer, you might not be paying the fee – but those still count toward your VAMP ratio. It's critical you know about them so you can identify the fraud pattern and stop it.

Transparency with data also fosters better trust and cooperation between you and your acquirer: it shows you're willing to tackle issues if you're made aware. If your acquirer doesn't offer a robust reporting portal, push them for it or find third-party tools to aggregate this data.

06. Evaluate your fraud prevention tools (and team).

Take stock of the tools and processes you use for fraud prevention.

- Are you relying solely on manual reviews or basic rules?
- Are you using an outdated fraud engine?

VAMP's advent might justify investing in more advanced solutions – like an AI-driven fraud platform, device fingerprinting, or multi-layered defense system – that can adapt quickly to new fraud vectors. If you're using a fraud service through your acquirer, find out if it's being updated for VAMP (some acquirer-provided tools might automatically route more transactions to 3-D Secure now, for instance).

If you use a third-party fraud provider, ask them directly how they can help clients stay below these new thresholds. Do they offer features like direct integration of chargeback data (to analyze what slipped through) or post-transaction monitoring to catch fraud signals before disputes happen?

Make sure your solution can handle enumeration attacks as well – not all fraud systems specifically look at high-volume auth attempts, so you might need additional rules or services to spot those. Importantly, assess if your team has the bandwidth and expertise to adjust fraud strategies on the fly. If not, consider getting external consulting or managed services to fine-tune your fraud setup for this new era.

07. Consider leveraging 3-D Secure (3DS where appropriate.

Under PSD2 in Europe, many merchants are already using 3-D Secure authentication extensively (or Transaction Risk Analysis exemptions) to manage fraud. In other regions, 3DS adoption is spottier due to fears of checkout friction.

However, 3DS can be a powerful tool to lower fraud and shift liability: when a transaction is fully authenticated via 3-D Secure, the issuer typically can't file a fraud chargeback against the merchant. That means fewer fraud disputes counting against you (though note, issuers could still file non-fraud disputes like "Service not received").

Visa's tougher stance might tip the scales in favor of using 3DS more, even in markets like the US. Merchants should weigh the fraud reduction benefits vs. the potential conversion impact. Modern 3DS2 implementations, combined with risk-based step-up (only challenging high-risk transactions), can actually be quite seamless for customers. If fraud is a big chunk of your dispute problem, the "friction" of a challenge might be far less costly than the VAMP penalties or lost revenue from fraud. Essentially, either you invest in fraud prevention (which might include 3DS, better data checks, etc.), or you might be forced to by your acquirer later – better to control that decision yourself.

08. Revisit your internal fraud/cost tolerances.

Use this moment to recalculate the true cost of fraud and chargebacks to your business.

Many merchants historically treated some fraud/chargeback losses as a "cost of doing business" and optimized for sales growth. The landscape is shifting – those costs now carry additional penalties and jeopardize your payment acceptance capabilities.

Build a model: for each dollar in fraud or dispute, consider not just the lost goods and chargeback fees, but now an extra $8 (if you're in VAMP) and potential lost sales if your acquirer raises your rates or terminates you.

The calculus may show that investing more in prevention yields a strong ROI. At the same time, set fraud thresholds and KPIs for your team that align with the new reality. If previously a 1% chargeback rate was acceptable, maybe now you target 0.5% to stay safe. Communicate these goals internally and allocate resources (budget for tools, headcount for review team, etc.) accordingly. Being compliant with card network rules also means protecting your bottom line – often, reducing fraud and disputes saves you money in the long run, even aside from avoiding VAMP fees.

By following the above steps, merchants can drastically lower their chances of ever being swept into the VAMP program. The overarching theme is proactive management: **don't wait for Visa or your bank to tell you there's a problem**. Continuously monitor, adjust, and collaborate to keep your dispute metrics in the clear.

How Can Acquirers (and PSPs) Prepare?

Acquirers and payment service providers face perhaps an even bigger mandate to adapt under VAMP.

Here are some actionable steps for acquirers to consider:

01. Assess your merchant portfolio risk.

Perform an audit of your merchants' current dispute and fraud rates under the new VAMP calculations.

- **Identify which merchants would be "Excessive"** if VAMP were in full effect today (≥2.2% dispute ratio, ≥1500 disputes) and which are approaching that.
- **Pay special attention to merchants in traditionally high-risk verticals** such as online travel, gaming, digital subscriptions, electronics, aggregator marketplaces, etc. – as well as any merchant that had high fraud write-offs or chargeback programs in the past.

This assessment will help you gauge how close your overall portfolio is to the 0.5% or 0.7% acquirer thresholds. If you discover that a handful of merchants are contributing a large share of disputes, you can prioritize those for remediation.

Also consider your "ideal customer profile" going forward: are there industry segments you might need to avoid or impose conditions on because their dispute rates could threaten your compliance? Some acquirers may decide to exit or not enter certain high-chargeback industries as a strategic choice under VAMP.

02. Strengthen your fraud prevention offerings.

As an acquirer, you should evaluate whether your current fraud monitoring infrastructure is up to the new task.

Many acquirers historically left fraud prevention to the merchant or offered basic tools. Now, because the acquirer is liable for portfolio performance, it may be wise to invest in better fraud and risk technology at the acquirer level. This could mean partnering with advanced fraud solution providers or enhancing your in-house risk systems. For example, deploying an AI-driven transaction scoring system across all merchants could help identify fraud spikes in real time.

Some acquirers will choose to mandate certain fraud controls: e.g. requiring merchants over a certain fraud rate to use 3-D Secure on all transactions, or to adopt specific tools (like card testing detection solutions). While merchants might resist one-size approaches, the acquirer has to balance portfolio safety with merchant flexibility. Offering value-added fraud prevention services (possibly for a fee) could turn this into a win-win: you help merchants reduce fraud (keeping both of you compliant) and create a revenue stream or loyalty point. In any case, not upgrading your fraud toolkit is risky – hoping each merchant manages on their own may not cut it when one rogue player can drag you into enforcement.

03. Engage with solution providers and networks.

Proactively reach out to all your relevant providers – fraud management vendors, chargeback management companies, your Visa reps, etc. – to discuss VAMP changes.

Ask your vendors:

- **What updates are you making to help us comply with VAMP?** For instance, if you use a chargeback alert service, can they now cover all dispute types (not just fraud)?
- **Can they feed data into a central dashboard** so you can monitor ratios in real time?
- If you use a gateway or processor, **do they support the new Visa Merchant Purchase Inquiry (VMPI)/Order Insight** for streamlined dispute resolution?

Ensure that the technology you have (or can integrate) will support key tasks: real-time dispute tracking, automated alerts when thresholds are at risk, and robust reporting for internal and Visa use.

On Visa's side, keep close communication with your Visa Risk Manager contacts. They can provide guidance and perhaps early warning data if they see trends in your portfolio. Some acquirers have access to Visa's risk portals; make sure you're leveraging those. Essentially, treat VAMP as a project that involves your whole ecosystem of partners – get everyone aligned on the goal of keeping your metrics low.

04. Improve merchant communication and data sharing.

Now more than ever, it's critical to share information with your merchants to jointly combat disputes.

If in the past you withheld certain dispute data (for example, fraud chargebacks that you absorbed liability for, or pre-arbitration alerts), consider providing that data to merchants in a useful format.

When merchants see the full picture of their fraud and disputes – even those they didn't "pay" for – they can adjust their controls to prevent recurrence.[47]

Also, educate your merchants about VAMP. Many merchants (especially smaller ones) might not be aware of these changes. Publishing a guide (much like this one) or holding webinars for your merchants can turn a compliance exercise into a value-added service. It demonstrates that as an acquirer you are proactively helping them stay compliant, not just penalizing them after the fact.

Some acquirers have started sending monthly "scorecards" to merchants, showing, for example, "Your VAMP ratio this month was X%, industry average is Y%, here are suggestions to improve." Such transparent communication can motivate merchants to act before things escalate.

05. Plan for customer experience impacts.

Recognize that efforts to reduce fraud and disputes often introduce friction in the payment experience.

For example, requiring 3-D Secure or adding identity verification steps will inevitably affect some genuine customers. As an acquirer, think about how you can support merchants in balancing security and user experience. Perhaps you can provide A/B testing tools for merchants to try 3DS on a subset of traffic, or analytics to show the cost of fraud vs. lost sales.

Also, consider your stance if merchants push back. Some may say, "We don't want to add friction, we'll just pay the fees." Under VAMP, that approach can hurt you too, so be ready to enforce changes if needed. It's a delicate dance: you want to keep your merchants happy (they are your customers, after all), but you also need them to comply.

One way to reconcile this is to frame compliance measures as protecting their business as well. For instance, remind merchants that being in VAMP can lead to account termination – it's not just fees, it's their ability to accept Visa at stake.[56] Helping them see the bigger picture can enlist their cooperation in tougher anti-fraud steps, even if it means slight checkout changes.

In short, acquirers should be proactive, collaborative, and strict when necessary.

Those who take a hands-on approach – guiding merchants, investing in technology, and keeping a close eye on metrics – will navigate VAMP successfully.

Those who remain passive risk sudden enforcement, unhappy merchants, and reputational damage with Visa.

As Visa's program intends, the future belongs to acquirers who are partners in risk management with their merchants.

VAMP Enforcement and Fees: What's at Stake?

It's important to understand the penalties and outcomes if you do end up in Visa's monitoring program under VAMP.

Enforcement fees per incident

Visa's new fee structure under VAMP is straightforward:

- Merchants identified as "Excessive" (above the dispute threshold) will be charged **$8** for each fraudulent or disputed transaction each month they are in the program.[17]

Acquirers will be charged

- **$4 per dispute** at the Above Standard level,
- **$8 per dispute** at the Excessive level.[18]

These fees are on top of normal chargeback fees or fines. They can change over time (Visa reserved the right to adjust them), but these are the figures as of 2025. There are no fees for an "Early Warning" status because, as noted, there is no early warning tier for merchants and the acquirer early warning is handled via notifications rather than fees.

No one wants to pay these fees – they directly erode margins. Many acquirers will pass the $8 fee right on to the offending merchant (and potentially tack on additional penalties of their own). So a merchant could effectively end up paying >$8 per chargeback in extra fines, in addition to the lost sale and typical $15–$30 chargeback admin fee.[57]

Grace period for first timers

Visa is offering a grace period of 3 months for first-time offenses in a rolling 12-month period.[12] This means if a merchant (or acquirer) is flagged into VAMP Excessive for the first time, Visa will notify them but not assess fees for three months.

This is intended to give a chance to fix the issues. However, note that this is a one-time mercy – if you drop out of the program and then re-enter a few months later, you likely won't get another grace period. Also, "grace period" doesn't mean consequence-free: the clock is ticking to reduce your ratios, and acquirers may still impose their own requirements during this time. Essentially, it's Visa saying "we'll hold off on penalties briefly, but get your act together fast."

If after three months the ratios are still excessive, fees will start hitting from month four onward. And if the issues persist over multiple cycles, Visa can escalate enforcement (longer monitoring periods, mandatory action plans, etc.).

Possible termination and other sanctions

The worst-case scenario for non-compliant merchants is not just fees – **it's losing the ability to accept Visa cards entirely.** Under the longstanding rules, card networks (via acquirers) can terminate a merchant that poses excessive risk or doesn't improve under a monitoring program.

While this is rare and a last resort, merchants that ignore repeated warnings could be headed toward an account termination.[46] This is essentially a death blow for most businesses, given Visa's market share (roughly 40% of global card transactions).

Acquirers, too, could face sanctions if they consistently fail to manage their portfolio – in extreme cases, Visa could levy hefty fines on an acquiring bank or restrict them from onboarding new merchants until issues are resolved.

Another consequence short of termination is required reserves: an acquirer might demand that a high-risk merchant hold a large deposit or rolling reserve to cover potential chargebacks.[46] This ties up the merchant's cash and can be quite painful.

In summary, the stakes are high. Fees might be seen as a cost of doing business by some, but the ancillary effects – reputational damage, stricter contract terms, loss of banking relationships – make being in VAMP a situation to avoid at all costs.

Relationship repercussions.

As noted earlier, VAMP is likely to reshape acquirer–merchant relationships.[50]

- **Acquirers** will be quicker to act against a merchant that endangers their standing, which could mean:
    - More frequent account reviews.
    - Higher scrutiny for new merchants during underwriting.
    - Less tolerance for merchants who push the envelope (e.g. marketing practices that lead to disputes).
- **Merchants**, for their part, might feel more "policed" by their payment partners.

Trust and communication will be key to not sour these relationships. But merchants should understand that if they slip into VAMP territory, their acquirer might start treating them like a high-risk account: think higher fees, holdbacks, or requests for a remediation plan.

The best way to maintain a positive partnership is to stay off Visa's radar by diligently self-managing fraud and disputes. That keeps the power in your hands rather than your acquirer's.

How FraudNet Can Help You Meet VAMP Requirements Now

The new VAMP standards are challenging, but the good news is that solutions exist today to help both merchants and acquirers immediately adapt to these requirements. FraudNet is one such solution – an advanced fraud detection and compliance platform that can directly address the pain points introduced by VAMP.

Here's how FraudNet can help:

01. Real-time fraud blocking to prevent disputes at the source.

FraudNet employs AI-driven, real-time transaction scoring to stop fraudulent transactions before they are approved. This is critical under VAMP. By intercepting fraudulent orders up front, you prevent the downstream effects (no authorization means no TC40 fraud report, and no chargeback).

FraudNet's engine analyzes hundreds of signals within ~100 milliseconds[58], allowing merchants to automatically decline high-risk payments or route them for further verification. This dramatically lowers the volume of fraud-related disputes. As Visa put it, VAMP is about catching fraud before it happens, and FraudNet is built to do exactly that.

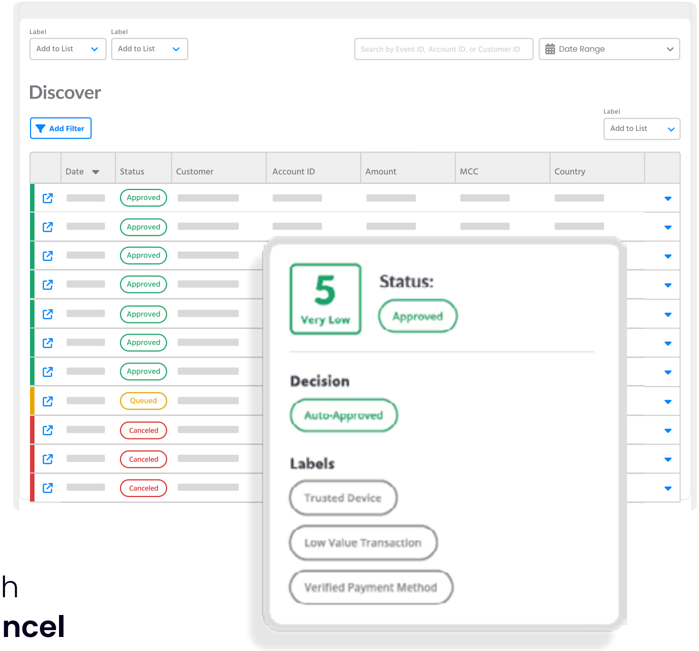
02. Card testing (enumeration) detection and mitigation.

FraudNet's monitoring can identify patterns characteristic of enumeration attacks, such as a sudden surge in authorization attempts, sequences of card numbers, or repetitive small-value declines. When such patterns are detected, FraudNet can automatically trigger defenses – for example, issuing a CAPT/challenge to the suspect traffic, slowing down the transaction rate, or blocking the source outright.

By preventing enumeration attacks, FraudNet helps merchants avoid tripping the 20% card-testing ratio threshold. These attacks are often carried out by bots, and FraudNet's device intelligence and behavioral analytics excel at spotting bot behavior. Stopping these attacks not only protects your VAMP metrics, but also spares you from other fraud that those tested cards would lead to.

03. Pre- and post-authorization scoring for full coverage.

FraudNet can operate at multiple points in the transaction lifecycle. It provides pre-authorization risk scores to catch fraud before payment authorization, and it can also score transactions in a post-auth monitoring mode. Post-auth monitoring is useful for catching fraud signals that emerge right after an order is placed (for instance, a customer calling to change the shipping address to a high-risk location might indicate the order was fraud).



Label: Add to List | Label: Add to List | Search by Event ID, Account ID, or Customer ID | Date Range

Discover

Add Filter | Label: Add to List

	Date	Status	Customer	Account ID	Amount	MCC	Country
		Approved					
		Approved					
		Approved					
		Approved					
		Approved					
		Approved					
		Approved					
		Queued					
		Canceled					
		Canceled					
		Canceled					

5 Very Low

Status: Approved

Decision: Auto-Approved

Labels: Trusted Device, Low Value Transaction, Verified Payment Method

If FraudNet flags a transaction post-auth as suspicious, **you could proactively cancel or refund it before it becomes a chargeback or fraud claim**. This approach addresses the issue of TC40 vs. chargeback double-counting – if you can act on a fraud indicator immediately post-purchase (perhaps even alert the issuer or cardholder), you might prevent a fraud report or chargeback from being filed.

Traditional fraud tools often stop at authorization, but FraudNet's continuous monitoring means fraudulent activity can be caught and mitigated even after initial approval, giving an extra layer of protection against those "two strikes" incidents. Crucially, FraudNet offers this end-to-end coverage without additional per-transaction costs – you're empowered to screen transactions as many times as needed to ensure nothing slips through.

04. Policy Monitoring and VAMP ratio tracking.

Beyond pure fraud prevention, FraudNet includes robust policy compliance monitoring features (sometimes referred to as Policy Monitoring in the platform). This is directly aligned with VAMP. It provides a real-time view of your dispute and fraud counts, calculating your effective VAMP ratio as you go. You can set custom alerts to notify you if, say, your ratio exceeds 1.0% in a given week – allowing you to take action before it exceeds 2.2%[59,60].

FraudNet's **Policy Monitoring** can ingest TC40 data, chargeback data, and authorization data to give a consolidated view. It also employs anomaly detection to catch unusual patterns (e.g. a spike in disputes or a cluster of fraud reports from one BIN) that might indicate a brewing issue[61]. By having this oversight, acquirers using FraudNet can manage their merchant portfolio in one place, and merchants can keep a close eye on their standing with Visa. Essentially, FraudNet can function as your VAMP early-warning system, something Visa itself isn't providing merchants directly.

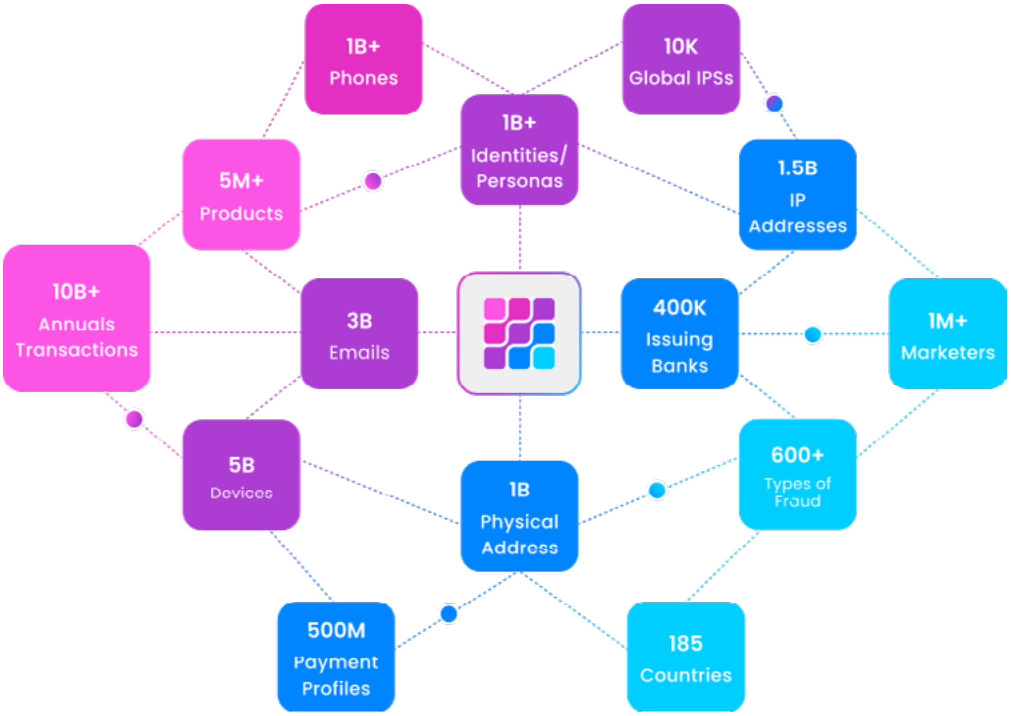
05. Automated case management and response.

When FraudNet identifies a risky transaction or a policy breach, it can automatically kick off workflow actions. For example, it can cancel orders, notify fraud investigation teams, or send data to fill out Visa's required documentation. If a merchant does end up in VAMP, having a tool like FraudNet means you can demonstrate to Visa and your acquirer that you have active controls and a remediation plan in place.

The platform's case management module lets you track fraud incidents and their resolutions, which is useful if Visa requests a remediation report. Plus, by automating many responses (like instant blocking of confirmed fraud or automatic refund on a dispute alert), it minimizes the operational burden on your team during critical moments[62,63]. This is key because Visa's program expects quick action – automation ensures you don't waste those grace period months doing things manually.

In summary, FraudNet empowers both merchants and acquirers to tackle VAMP head-on. It stops the kinds of activities (fraud and enumeration) that VAMP penalizes, and it provides the real-time visibility and control needed to stay within thresholds. Importantly, it's a solution that can be deployed immediately. With VAMP enforcement live now, merchants and acquirers can't afford lengthy development cycles or half-measures.

FraudNet's platform is ready out-of-the-box to help you meet the new standards from day one. Whether it's preventing "double jeopardy" from fraud chargebacks or giving you peace of mind through continuous monitoring, **FraudNet is designed to keep your business compliant, secure, and a step ahead of fraudsters.**



Why Did Visa Change These Programs?

Visa's overhaul of its dispute monitoring programs with VAMP is driven by several factors:

01. Rising fraud and dispute trends

The payments ecosystem has seen significant increases in fraud and chargebacks in recent years, especially in card-not-present channels. The growth of e-commerce, the pandemic-accelerated shift to digital, and new fraud tactics (like enumeration attacks) have all contributed.

Visa cited that enumeration (card testing) alone leads to $1.1 billion in fraud losses annually. Separately, consumer disputes of transactions have grown – in the U.S.,[14] cardholders disputed about $11 billion worth of charges in 2022, up from $7.2B in 2019.[14] Friendly fraud (first-party misuse) has become a dominant share of chargebacks (around 3 in 4 disputes by some Visa estimates).[29] With fraud and disputes on the rise, Visa recognized that the old programs (VDMP/VFMP) might not be sufficient to curtail the problem.

VAMP is an attempt to simplify the system and cast a wider net to catch more of this unwanted activity. In fact, Visa projected that the new VAMP could address **4× more fraud globally** – about $2.5 billion in losses – compared to the previous programs.[64] By unifying fraud and chargebacks into one measure, Visa is essentially saying: "a problem is a problem, no matter the type," thereby addressing more total incidents.

Fraud in Numbers

Card Testing Losses

$1.1B

In **2022** U.S. cardholders disputed

$11B

in transactions

Friendly Fraud

or first-party misuse has become a dominant share of chargebacks (3 in 4 by some Visa estimates).

02. Evolving payments and new attack vectors

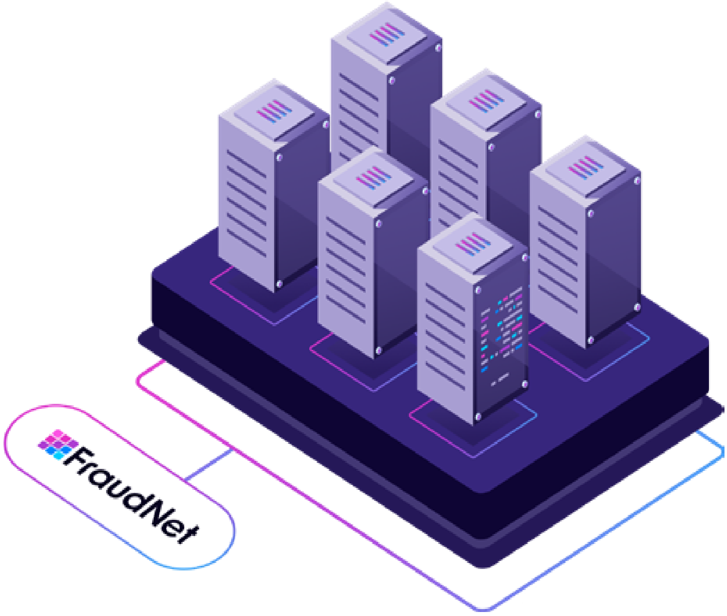
The landscape of payments is very different than when VDMP/VFMP were introduced. We now have real-time payments, digital wallets, automated agents, and commerce driven by AI – complexity has increased.[65,66] Fraudsters have gotten more sophisticated, leveraging automation (bots) and large-scale testing.

Visa likely saw that focusing only on fraud chargeback rates (VFMP) missed things like card testing, and focusing only on chargeback rates (VDMP) missed the early warning signs of fraud. The new program addresses these "gaps" – enumeration being explicitly added, and fraud alerts (TC40s) being counted to catch issues before they fully manifest as chargebacks.

It's a move from a reactive approach to a more proactive, preventive stance.[66]

Visa wants to "make it harder for fraud to be committed in the first place," as their executives have said,[66] and part of that is forcing stakeholders to act on fraud signals sooner.

03. Regulatory and ecosystem alignment



Especially in regions like Europe, **regulators have pushed for lower fraud rates** (PSD2's RTS on SCA, for example, effectively forces most transactions to have fraud below 0.1–0.2% for certain exemptions).

Visa's program aligns with these goals by pressing the industry to lower fraud. Some analysts see VAMP as Visa bringing its own rules up to par with regulatory expectations – for instance, the elimination of the high "standard" thresholds and focusing on risk-based compliance echoes how regulators expect continuous risk management rather than occasional penalty fees.

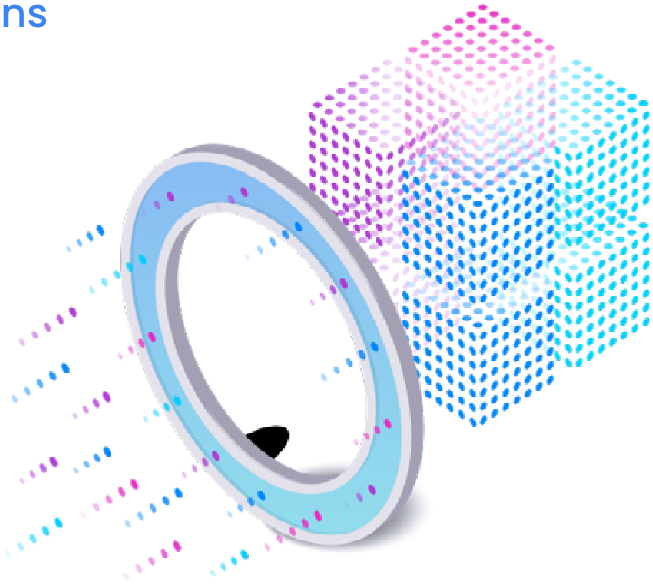
Additionally, by consolidating programs, Visa is making it easier for merchants and acquirers to understand what's expected globally, rather than juggling different regional rules. This simplification can improve compliance. Visa also likely considered feedback from clients: running three separate programs (VDMP, VFMP, GBPP for gross fraud in some regions, etc.) was administratively heavy. One unified program reduces confusion and is more straightforward to administer, both for Visa and for banks/merchants.

04. Encouraging adoption of Visa tools and best practices

It's worth noting that Visa stands to benefit when clients adopt certain tools. VAMP's initial design (later tweaked) offered exclusions for those using Visa's Verifi and RDR services, which could be seen as an incentive to use Visa's dispute resolution products. While they modified the details, it still highlights that Visa is encouraging merchants to embrace solutions like RDR, Order Insight, Compelling Evidence 3.0, etc. that ultimately reduce disputes in the system.

Similarly, by penalizing enumeration, Visa pushes merchants to use its intelligence feeds (VAAI) and invest in bot mitigation – which in turn protects Visa's network integrity. So, part of the "why" is that **Visa is nudging the ecosystem toward certain technologies and practices that they believe will strengthen overall security** (and, cynically, that can also include Visa-branded services).

05. Flexibility and fairness considerations



The shift to risk-based enforcement and the elimination of blanket fines also reflect Visa's acknowledgment that a one-size approach can be unfair. In the past, a merchant breaching a threshold by a tiny amount might face hefty fines, while a more egregious case paid the same fine – not exactly equitable.

The new approach, with fees proportional to the number of disputes and with collaborative remediation, is more flexible. It gives leeway to clients with marginal issues and focuses attention on the serious outliers.

Visa likely believes this will engender more cooperation rather than adversarial reactions. They even stated the program is designed to accommodate "varying levels of risk appetite" among clients[26] – meaning, if an acquirer has thought it through and is willing to accept higher risk (perhaps for higher fees), the program can accommodate that to an extent, so long as it's managed.

In essence, Visa is updating its approach to keep pace with a changing world: more digital transactions, cleverer fraudsters, and a need for a cleaner payments ecosystem to maintain trust.

By doing so, Visa protects its brand (cardholders expect Visa to be safe), helps issuers (fewer fraud losses), and arguably helps merchants and acquirers in the long run by reducing overall fraud which can improve approval rates and customer experience.[53] Of course, in the short term, it means some pain for those who need to adjust – but the end goal Visa envisions is "higher authorizations, higher approvals driven by lower fraud and disputes",[67,53] **which benefits everyone in the payment ecosystem.**

In Summary

Visa's new VAMP program changes how the payments industry handles fraud and disputes.

To recap, here are the key points and what businesses should do.

Simplification with Stricter Standards

Visa has combined three programs into one, making compliance easier with just one ratio to check. However, **the new rules are tougher and cover all disputes and fraud cases**. Smaller merchants may find some relief, but larger businesses will face more scrutiny.

Targeting Significant Volumes

VAMP focuses on merchants and acquirers with large transaction volumes, setting a **minimum of 1,500 disputes**[40]. This targets major sources of fraud and disputes, impacting large e-commerce merchants and payment processors while giving smaller businesses some flexibility.

Encouraging Proactivity and Collaboration

Visa stresses the need for proactive risk management. **Merchants and acquirers should identify issues early to prevent fraud**. The program supports tools like fraud detection and encourages ongoing communication between merchants and acquirers. This partnership is key for successful compliance.

Global Standards and Alignment

VAMP starts in Europe but aims to expand globally, creating consistent standards for all regions. This benefits merchants in multiple markets and prepares them for future regulations. **Companies adhering to VAMP will be better positioned for global compliance.**

Merchants need to act quickly to manage fraud and disputes.

Invest in prevention, refine strategies, and communicate with your acquirer. Acquirers should support their merchants while maintaining a strong risk profile with Visa.

Acquirers must manage their portfolios effectively.

Support and educate your merchants, but be ready to make tough decisions regarding non-compliant ones. Maintaining a good risk profile with Visa is essential for your business.

By improving fraud prevention and fostering compliance, you can gain a competitive edge—merchants will choose acquirers who help them stay out of trouble.

Exciting times are ahead with VAMP, Visa's initiative aimed at creating a safer payments ecosystem. By effectively tackling fraud and disputes, VAMP delivers significant benefits, including lower fraud losses and a smoother consumer experience. Merchants and payment providers who adapt quickly can avoid extra fees, reduce fraud costs, and build customer trust. If this seems daunting, partnering with the right technology provider can help.

FraudNet provides a comprehensive solution to monitor and mitigate risks associated with VAMP, including preventing fraud and tracking disputes in real-time. With enforcement starting in October 2025, now is the time to reassess your strategies.

Take proactive steps today. Whether you enhance internal practices or use FraudNet's platform, securing payments and ensuring compliance are essential. This will not only satisfy Visa but also strengthen your business's reputation.

Need guidance on these changes? The dedicated team at FraudNet is ready to assist. Reach out for a consultation or demo, and let's work together to ensure your business thrives in this new payment landscape.

Learn More

Endnotes

[1] [11] [26] [33] [43] Visa's Acquirer Monitoring Program (VAMP): What to Know for 2025 - Midmetrics

[2] [3] [4] [6] [21] [22] [31] [32] [36] [37] [41] [49] Visa Acquirer Monitoring Program Fact Sheet (2025) - Visa.com

[5] [10] [12] [28] [30] [34] [35] [42] [44] [56] Visa Acquirer Monitoring Program (VAMP) - Chargeback Gurus

[7] [15] [16] [17] [18] [23] [24] [25] [27] VAMP Merchant Guidance - Trust Payments

[8] [9] [13] [29] [40] [45] [46] [47] [48] [50] [51] [55] [57] VAMP Enforcement October 1, 2025: Merchant Impact Analysis - Chargebacks911

[14] [19] [20] [64] Introducing the Visa Acquirer Monitoring Program - Visa

[38] [39] [53] [54] [65] [66] [67] Evolving the Visa Acquirer Monitoring Program - Visa

[52] Insight: The Visa Acquirer Monitoring Program (VAMP) - Kount

[58] Fraud Detection & Prevention - FraudNet

[59] [60] [61] [62] [63] Visa Acquirer Monitoring Program (VAMP) Compliance with Policy Monitoring - FraudNet