2026 Global eCommerce
Payments & Fraud Report

See survey results on:

— Payment acceptance
— Payment metrics and tactics
— Fraud management strategies and challenges
— Fraud management metrics and tactics
— Post-purchase fraud and abuse

VISA

MRC

Contents

© Visa 2026. All rights reserved.

Overview

The Merchant Risk Council [MRC], Visa Acceptance Solutions, and Verifi are pleased to share the results of our latest Global eCommerce Payments & Fraud Survey. The purpose of this report is to convey fact-based, transparent research on merchants' perceptions of various key trends and challenges in the realm of eCommerce payments and fraud.

This year's report is based on a global survey of more than 1,200 eCommerce merchants, which was fielded by the independent research firm B2B International in November and December 2025. The survey sample includes a diverse mix of small-business [SMB], mid-market, and enterprise merchants representing organizations based in more than 35 countries spanning North America and Europe as well as the Asia-Pacific [APAC] and Latin America [LATAM] regions. In addition to the results from this year's survey, we also leverage trended survey data from previous years in this report to understand not just how merchants are thinking about various topics and trends today but also how their views have been changing as the eCommerce payments and fraud landscapes have evolved over time. The next section of the report contains additional details on the survey methodology and sample.

This year's report is based on our global survey of over 1,200 eCommerce merchants, which was fielded by the independent research firm B2B International in November and December of 2025.

Leveraging our robust survey dataset, this report delves first into the eCommerce payments landscape to shed light on two key topic areas: payment acceptance and payment metrics and tactics. Following the two payments sections, the report shifts focus to three major topic areas pertaining to eCommerce fraud: fraud prevention strategies and challenges, fraud prevention metrics and tools, and post-purchase fraud and abuse. In addition to the five sections of detailed insights and analysis above, the report also contains an executive summary of key findings and takeaways upfront as well as a brief conclusion at the end, which we hope will help put all of the fresh, detailed data and insights conveyed throughout the report into broader context and perspective.

The MRC extends its gratitude to all its members who took part in the survey, to Visa Acceptance Solutions and Verifi for co-sponsoring the research, and to B2B International for managing the research, analysis, and development of the report.

© Visa 2026. All rights reserved.

Survey methodology & sample

The survey for this year's report was fielded from November to December of 2025. In total, 1,278 merchant professionals involved in eCommerce payment and fraud management (including 69 MRC members) completed the survey. The respondent sample includes fraud and payment professionals based in 37 countries spanning four major geographic regions, with broad representation across revenue tiers, sales channels, and eCommerce categories. The figures below show a breakdown of the sample by geographic region, merchant size (eCommerce revenue*), and eCommerce category.

Figure 1: Share of sample by region

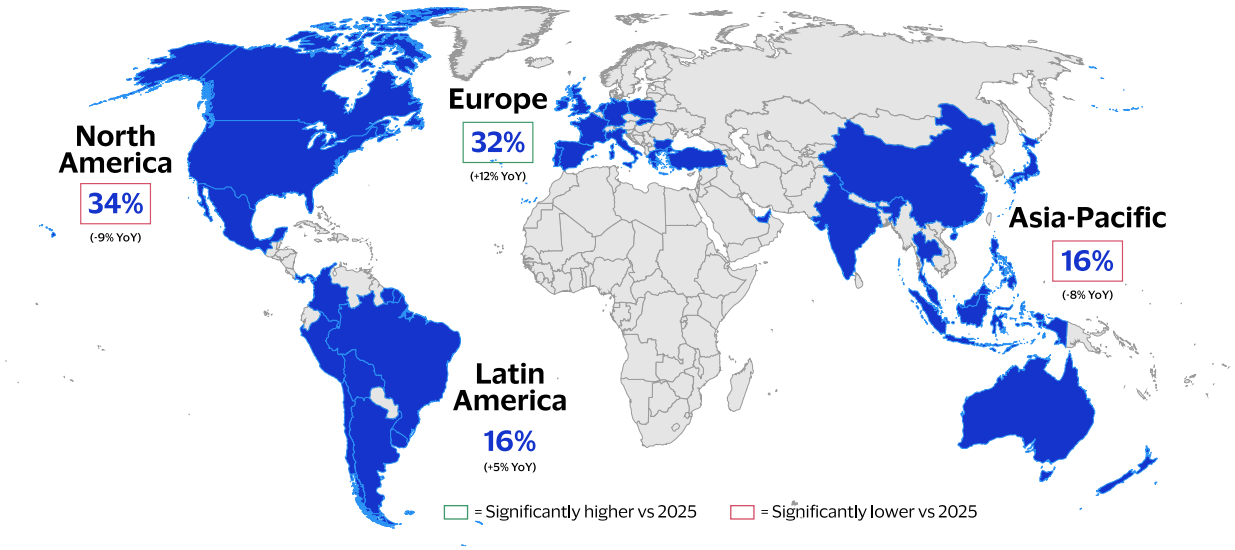


Figure 2: Share of sample by size (eCommerce revenue)

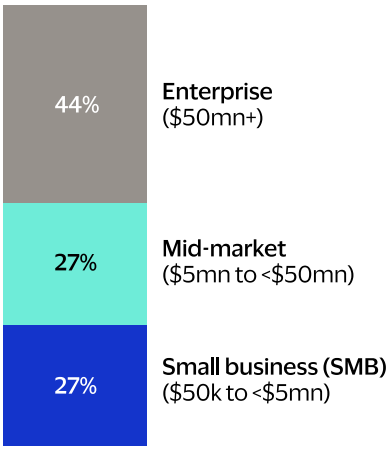
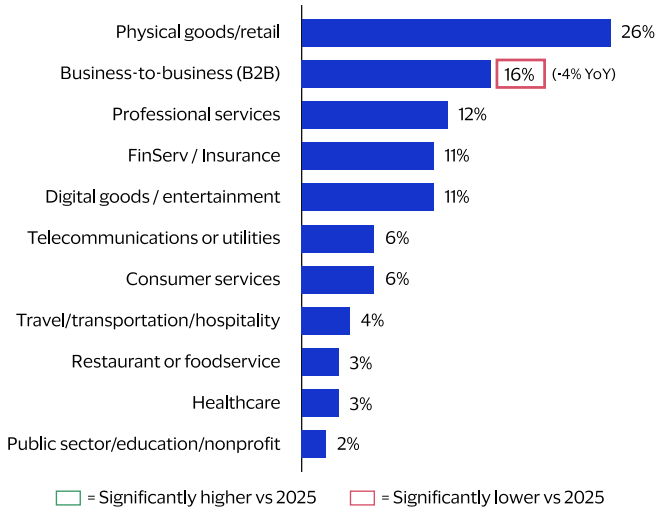


Figure 3: Share of sample by eCommerce category



It is worth noting that in addition to increasing the total sample by ~200 completes compared with last year, we also rebalanced the sample distribution in terms of geographic spread, increasing representation from merchants in Europe and Latin America and decreasing the share of sample based in North America and APAC compared with previous surveys. These shifts were implemented intentionally to ensure the scope and design of the research aligns with the core objective of capturing and conveying the perspectives of the entire global eCommerce merchant industry.

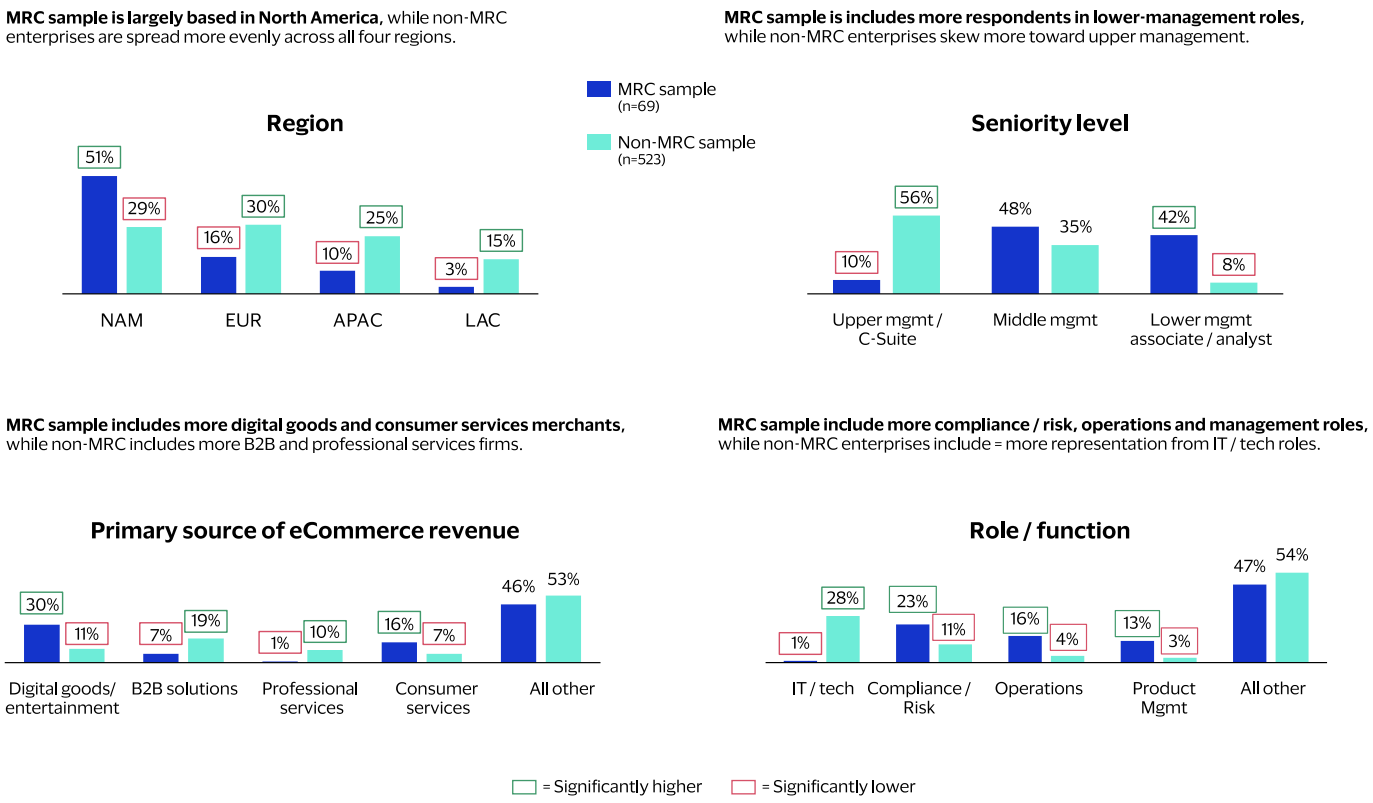
*Note: All currency values in this report are in U.S. dollars.

© Visa 2026. All rights reserved.

Survey methodology & sample

Among the 69 MRC members participating in this year's survey, roughly half (51%) are based in North America, with the remainder largely reporting in from Europe (16%). The majority (at least 61%) represent large enterprise merchants, i.e. those generating more than $50 million in annual eCommerce revenue. Because most MRC members are enterprise merchants, their survey responses are compared throughout this report with responses from non-MRC enterprises. When considering these comparisons, it is important to keep in mind the key differences in the makeup of these survey samples, which are summarized in Figure 4.

Figure 4: Differences in MRC member sample versus non-MRC enterprises



From an organizational perspective, MRC members in this year's survey are more likely to be based in North America and to sell digital goods and consumer services than non-MRC enterprises. In terms of individual demographics, the MRC sample includes more responses from lower-management roles and compliance/risk, operations, and product management functions, while the responses from non-MRC enterprises include more representation from upper management and IT/technology roles.

© Visa 2026. All rights reserved.

Executive summary

Detailed insights from the survey are organized into five sections in this report. The first two sections examine the state of **eCommerce payments**; the last three sections address trends and topics pertaining to **eCommerce fraud**.

In this section, we summarize the key themes and findings emerging from all five sections of the report, providing an overview of all the major changes, trends, and headlines uncovered in our latest research:

1. Payment acceptance

Real-time payments rise into five most widely accepted methods

- Merchants continue to accept a handful of different payment methods (four to five), on average. The majority accept cards, digital wallet payments, and bank transfers (direct debit), and nearly half (48%) take mCommerce mobile payments.
- Acceptance of real-time payments (RTP) continues to grow rapidly: 43% of merchants say they currently accept RTP in this year's survey—a 6% increase over last year—making this the fifth most widely accepted method globally.
- Among merchants not currently accepting RTP, nearly half (48%) say it is likely they will begin doing so within the next 12 months, suggesting that acceptance of RTP is likely to continue growing quickly over the course of 2026.

Agentic AI payments loom on the horizon, with most making plans for acceptance

- One of the new topics in this year's survey is agentic AI payments, which we define as eCommerce payments initiated by AI assistants or applications on behalf of human consumers. Currently, just 19% of merchants say they have a plan and solutions in place to accept agentic AI payments, roughly on par with the share currently accepting cryptocurrency (17%).
- Most merchants (63%) are actively exploring or implementing solutions to process agentic AI payments in the near future, with half of this group indicating they are in the midst of implementation. As with other emerging payment methods, enterprise merchants are leading adoption of agentic AI payments, with 28% indicating they already have solutions in place to accept them, versus just 12% of mid-market and SMB merchants.

19% of merchants have a plan and solutions in place to accept agentic AI payments.

2. Payment metrics and tactics

Payment success rate and revenue stand out as the top two KPIs

- Out of 14 payment metrics covered in the survey, merchants are significantly more likely to place the highest importance on payment success rate and revenue. The importance of these two above all others signifies that merchants fundamentally prioritize efficiency and profitability as paramount when assessing eCommerce payments.
- In addition, more than 70% rate each of the following seven metrics "very" or "extremely" important: authentication rate, authorization rate, loss rates (due to fraud and chargebacks), cost of service/cost per customer, order conversion rate, refund rate, and settlement time. So in total, there are at least 10 different types of payment metrics most merchants consider important for comprehensively measuring "success" in eCommerce payments from a financial, operational, and customer experience perspective.
- As in past years, MRC members and non-MRC enterprises exhibit starkly different views on the importance of various payment metrics. MRC members are far less likely than non-MRC enterprises to view customer NPS, retry performance, cost of service, settlement time, refund rate, and average ticket size as highly important.

© Visa 2026. All rights reserved.

Executive summary

Most employ payment tokenization and authorization-related tactics to enhance security, efficiency, and CX

- Almost three-quarters (72%) of merchants in this year's survey say they use one or more forms of payment tokenization, a significant year-on-year increase of 12%. This increase is partly driven, however, by our addition of customer tokens as a new option in this year's survey, along with gateway and network tokens. The data show broadly similar usage rates for all three forms of tokenization, with 40–45% of merchants, globally, saying they currently use each one.
- In addition to tokenization, merchants leverage an array of other advanced tools and tactics to maximize authorization rates on eCommerce payments, with intelligent payment routing and strong customer authentication (SCA) being the two most common (each used by four in ten merchants, globally). Use of these tactics varies across merchant sizes and segments (e.g., MRC members over-index on using 3D Secure 2 and automated retries), but overall, it's clear most merchants are pulling multiple levers to maximize their success in eCommerce payments (security, efficiency, profitability, and CX).

80%+ of merchants say data and technology are their biggest fraud management challenges.

3. Fraud management strategies and challenges

Cost concerns keep mounting, spurring merchants to prioritize profitability and pull back on spending

- The share of merchants citing "minimizing operational costs" as their top overall priority in fraud management rose significantly for the second year in a row. The share of merchants citing cost minimization as their primary imperative has tripled over this short period, climbing from 10% in 2024 to 29% this year. As more merchants focus first and foremost on limiting costs, fewer are prioritizing "reducing fraud & chargebacks" and "improving the customer experience."
- Merchants also cite "lack of internal resources (budget, staff, etc.)" as one of their biggest challenges in fraud management this year. The majority (52%) expect spending on staff and talent in this area to stay flat or decrease over the next two years, and nearly half (45%) say the same about spending on fraud management tools and technologies. Altogether, these data points paint a vivid picture of fraud management professionals being challenged to "do more with less" in terms of effectively thwarting the myriad fraud threats they face while spending less and saving more.

Data and technology is the main frustration and focus area for improvement

- While cost constraints pose difficulties, the biggest frustrations for merchant fraud management professionals are related to data & technology. Many struggle to access relevant data and to leverage it effectively for preventing and managing fraud. Others find it hard to continuously customize and orchestrate different anti-fraud tools and platforms so they function cohesively. And of course, these challenges are all compounded by the dynamic, rapidly evolving nature of eCommerce and payment fraud, in which new threats (such agentic AI fraud) emerge with exhausting frequency.
- Given the many pain points merchants are feeling with their fraud management data and tools, it is no surprise that this is also their primary focus area for improvements and investments. Improving the accuracy of AI- and ML-powered fraud tools and better orchestrating them to work well together, as well as increasing automation of fraud prevention, are all key focus areas for many merchants over the next one to two years.
- When considering future investments in this area, merchants will put a premium on efficiency gains, both in terms of cost savings and reduced time and labor. Most merchants tell us they are having to spend increased time on fraud prevention and management every year, while very few are seeing any time savings. As such, 62% agree that reducing time spent on fraud management will be a moderate or major factor in their future fraud management investments.

© Visa 2026. All rights reserved.

4. Fraud management metrics and tactics

Fraud incidence rates decline for a second consecutive year

- Reported incidence rates of all forms of eCommerce fraud decrease for the second consecutive year. Incidence of real-time payment fraud, coupon/discount abuse, and re-shipping show significant decreases compared with 2025.
- Merchants are still grappling with a formidable fraud threat, overall, as the average merchant reports 3.8 different fraud attacks per year. Five different fraud attacks impact at least one-third of merchants, globally: refund/policy abuse, real-time payment fraud, phishing/pharming/whaling, first-party misuse, and card testing. MRC members report a much larger variety of attacks than non-MRC enterprises, replicating a trend we see consistently in our survey data each year.
- Other fraud metrics remain largely unchanged, although fraud rate by order increased significantly (from 3.0% last year to 3.5% this year). False positives, or customer insults, may also be on the rise, as a significantly larger share of merchants reported higher rates for this particular metric in this year's survey compared with last year.
- Consistent with a long-running trend in our research, MRC members continue to report significantly better fraud metrics than non-MRC enterprises across the board.

Merchants are still grappling with a formidable fraud threat, overall, as the average merchant reports 3.7 different fraud attacks per year.

Usage rates for many fraud management tactics and tools decline slightly

- Survey data show declines in merchant usage of many fraud management tactics and tools, including fraud monitoring across the customer journey and use of various AI-/ML-powered fraud prevention tools.
- Merchants continue to shift away from manual screening of eCommerce orders and toward digital screening. Since 2024, the average share of eCommerce orders screened manually has declined significantly, from 25% to 21%, while the average share of orders screened digitally has increased from 51% to 54%.

5. Post-purchase fraud and abuse

Most merchants report an increase in first-party misuse over the past year

- More than six in ten merchants (64%) report increasing rates of first-party misuse (FPM), with one-quarter claiming increases of 25% or more. The average share of (total) fraudulent disputes believed to be FPM decreased significantly, falling to 17% (versus 20% in 2024 and 2025). Merchant estimates of the average cost to resolve each FPM dispute ticked upward for the third consecutive year, surpassing $80 for the first time in our research.

© Visa 2026. All rights reserved.

Executive summary

Most merchants report an increase in first-party misuse over the past year

- More than six in ten merchants (64%) report increasing rates of first-party misuse (FPM), with one-quarter claiming increases of 25% or more. The average share of (total) fraudulent disputes believed to be FPM decreased significantly, falling to 17% (versus 20% in 2024 and 2025). Merchant estimates of the average cost to resolve each FPM dispute ticked upward for the third consecutive year, surpassing $80 for the first time in our research.
- Merchants attribute increasing FPM primarily to consumers learning how to "game the system," as well as general increases in their eCommerce sales/orders. Compared with last year, significantly fewer merchants now ascribe responsibility for rising FPM to issuing banks (for making it fast and easy for consumers to submit disputes).

Use of compelling evidence declines slightly, but most still use it as one of many tools to combat FPM

- The share of merchants making use of compelling evidence decreased in this year's survey, but 83% still utilize this method to mitigate FPM disputes. Survey data also show a shift in the types of data used for compelling evidence, with more merchants sharing item and product information and fewer submitting customer device or account details.
- Merchants continue to employ a range of other anti-FPM tools and tactics, with several approaches seen as highly effective in countering this form of fraud, such as transaction monitoring, analysis of non-fraud chargebacks and declines, requiring card verification values (CVV) for card payments, checking customer purchase and order histories, and working with providers to prevent and identify fraudulent transactions.

83% of merchants still use compelling evidence to fight FPM, despite year-over-year declines and a shift toward item and product data over device or account details.

Refund/policy abuse remains rampant, posing a major challenge for merchants and payment partners

- Roughly six in ten (61%) report a rise in refund/policy abuse, with one in five (20%) citing a spike of 20% or more. A higher share of merchants cites significant increases (>5%) in this form of fraud compared with last year, while fewer are reporting flat or declining incidence rates.
- False claims of unreceived goods continue to be the most common form of refund/policy abuse impacting merchants, followed by returns of used, damaged, or incorrect items. Only 3% say they have not suffered any of the specific types of refund/policy abuse shown in the survey, a significant decrease from the 7% who reported no incidence in 2025.

© Visa 2026. All rights reserved.

Section 1:

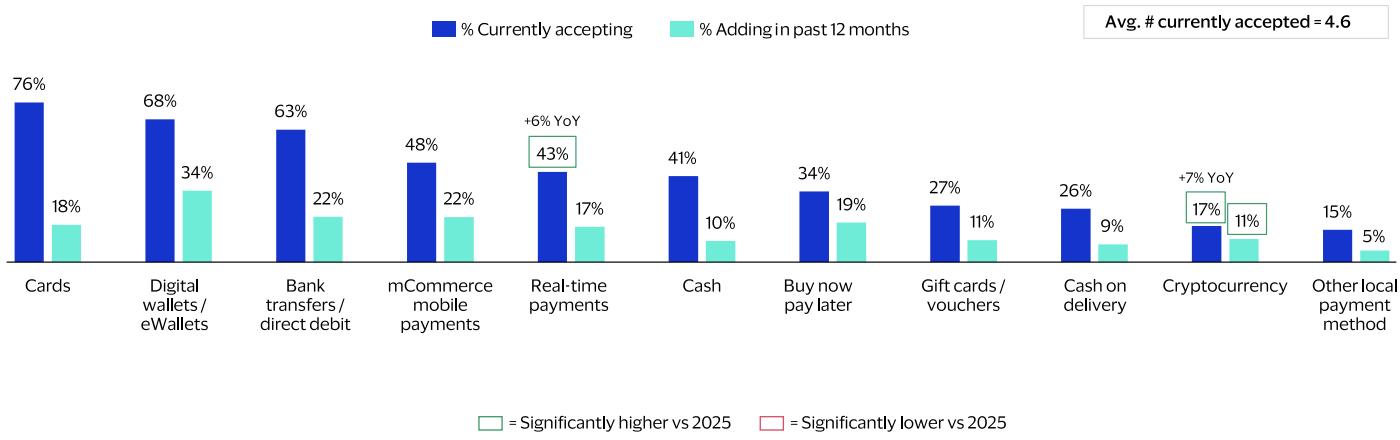
Payment acceptance

This section of the report offers insights into merchant payment acceptance for eCommerce customers, including which payment methods are currently accepted, as well as merchants' views and plans concerning new and emerging methods, like real-time payments and agentic AI payments.

Real-time payments (RTP) rise into the five most widely accepted methods

Survey data shows merchants currently accept four to five eCommerce payment methods, on average. Cards, digital wallets, and bank transfers top the list, each accepted by more than 60% globally (see Figure 5). Nearly half (48%) accept mCommerce payments, and 43% accept RTP, a significant year-on-year increase that elevates this method above cash and into the top five overall.

Figure 5: Payment methods currently accepted and added in past 12 months (2026, all payment professionals)



Also shown in Figure 5 are the percentages of merchants saying they added each payment method in the past 12 months, which gives insight into how quickly each method is being adopted and implemented within acceptance offerings. The methods with the highest adoption rates in the past year include digital wallets (34%), bank transfers (22%), and mobile payments (22%). Buy now, pay later (BNPL) methods are also growing quickly, with roughly one in five merchants (19%) adopting this option in the past year.

Acceptance offerings vary significantly based on merchant size, as illustrated by the data in Figure 6. In general, larger merchants accept more payment methods, with the average number ranging from 4.2 for SMBs up to 5.0 for enterprises. Methods that enterprise merchants are significantly more likely to offer include digital wallets, BNPL, and gift cards or vouchers. Notably, acceptance rates for RTP are similar across merchant sizes, indicating demand for these new options is strong across the board.

© Visa 2026. All rights reserved.

Section 1: Payment acceptance

Acceptance offerings vary significantly based on merchant size, as illustrated by the data in Figure 6. In general, larger merchants accept more payment methods, with the average number ranging from 4.2 for SMBs up to 5.0 for enterprises. Methods that enterprise merchants are significantly more likely to offer include digital wallets, BNPL, and gift cards or vouchers. Notably, acceptance rates for RTP are similar across merchant sizes, indicating demand for these new options is strong across the board.

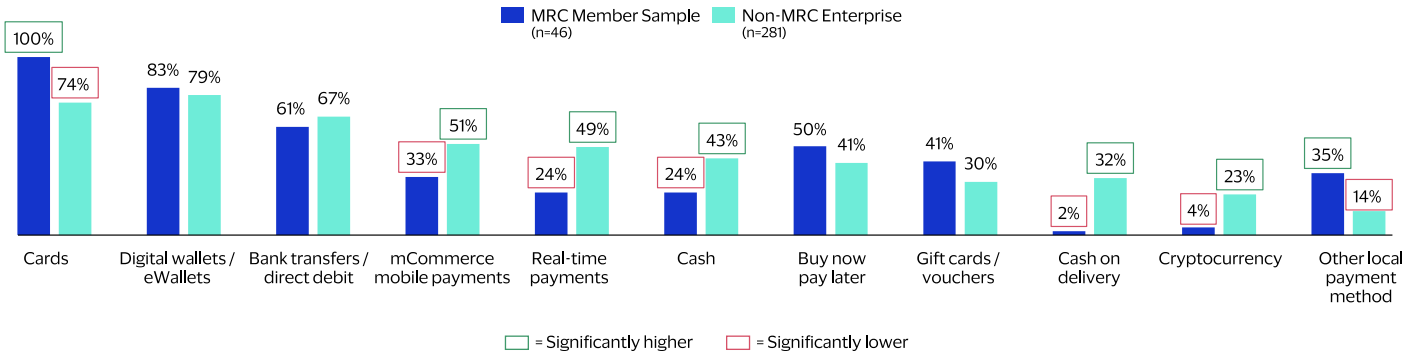
Figure 6: Payment methods currently accepted, by merchant size (2026, payment professionals)

	Overall	Merchant size		
		SMB	Mid-market	Enterprise
Base	*693*	*185*	*183*	*311*
Cards	76%	74%	77%	77%
Digital wallets / eWallets	68%	55%	63%	80%
Bank transfers / direct debit	63%	59%	64%	66%
mCommerce mobile payments	48%	47%	48%	49%
Real-time payments	43%	41%	40%	47%
Cash	41%	41%	43%	41%
Buy now pay later	34%	21%	34%	41%
Gift cards / vouchers	27%	25%	20%	32%
Cash on delivery	26%	21%	26%	29%
Cryptocurrency / stablecoins	17%	14%	15%	21%
Other local payment method	15%	17%	12%	16%
Avg. # of payment methods accepted	**4.6**	**4.2**	**4.4**	**5.0**

= Significantly higher vs. other segments = Significantly lower vs. other segments

There are also significant differences between the payment acceptance offerings of MRC members and non-MRC enterprises (see Figure 7). Acceptance of card payments, for instance, is universal among MRC members in this year's survey, while only three-fourths (74%) of non-MRC enterprises accept such payments. MRC members are also more likely to accept BNPL, gift cards/vouchers, and alternative, local payment methods (such as Pix and Boleto). Non-MRC enterprises report significantly higher acceptance rates for mCommerce mobile payments, RTP, cash/cash-on-delivery, and cryptocurrency payments.

Figure 7: Payment methods currently accepted, by MRC membership (2026, payment professionals)



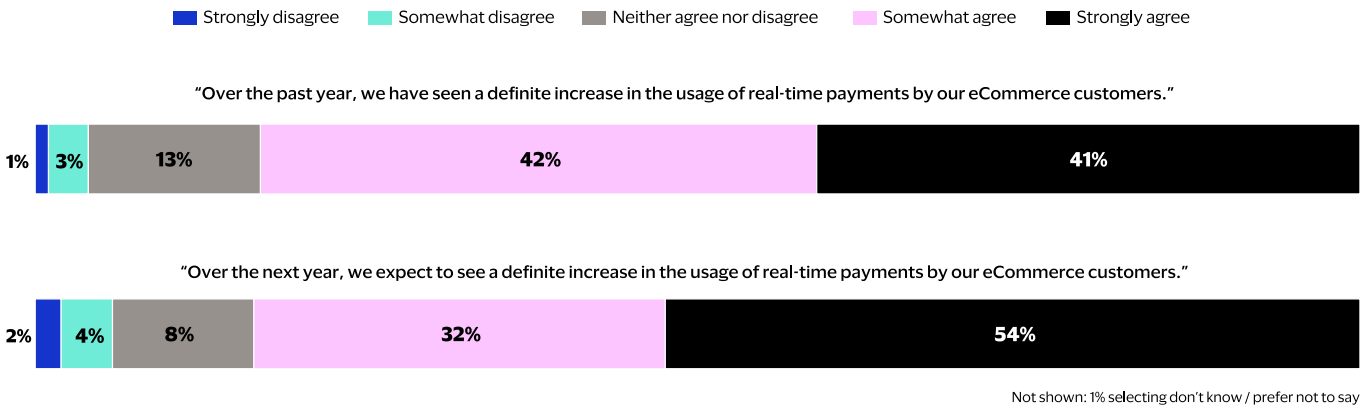
© Visa 2026. All rights reserved.

Section 1: Payment acceptance

RTP set for further growth in 2026 given strong uptake among merchants and consumers

Additional data from the survey suggest there will continue to be rapid adoption of RTP in 2026. RTP-accepting merchants report strong uptake among customers, with 83% seeing "a definite increase in the usage of real-time payments" over the past year, and 86% expecting this growth to persist over the next 12 months (see Figure 8).

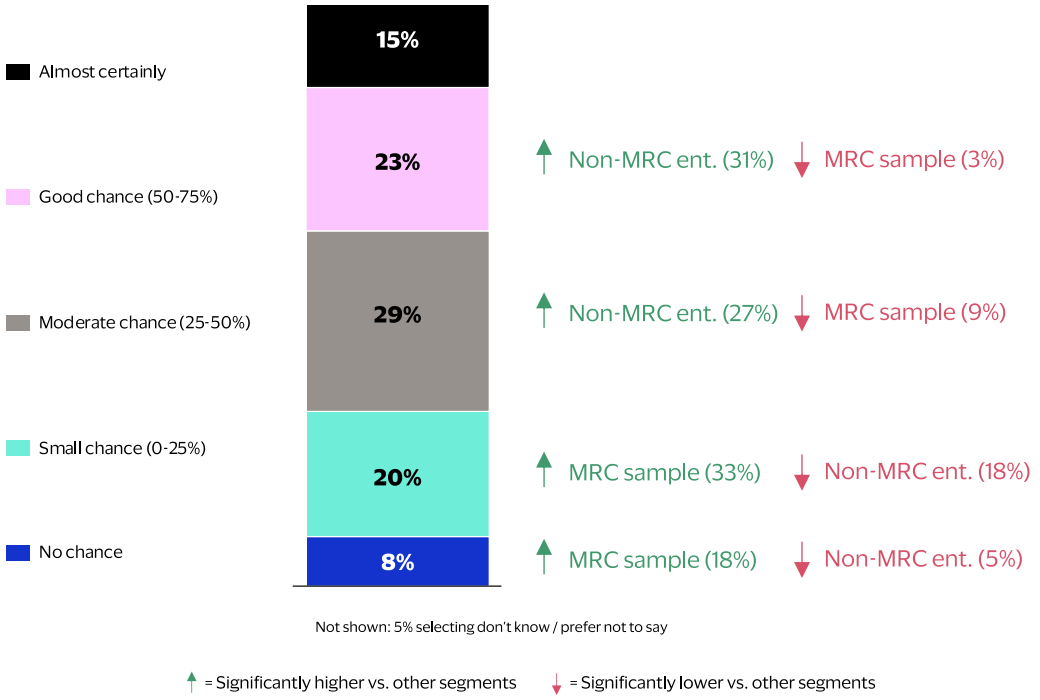
Figure 8: Merchant views on customer usage of real-time payments (2026, payment professionals currently accepting RTP)



Not shown: 1% selecting don't know / prefer not to say

Among the 57% of merchants that do not currently accept RTP, nearly four in ten (38%) say there is a high likelihood they will add it in the next year (see Figure 9). And another 49% of this group say there is at least a small or moderate chance of adding this acceptance method. Only 8% of non-RTP-accepting merchants indicate "no chance" of implementing this in the next 12 months.

Figure 9: Likelihood of adding real-time payments (2026, payment professionals not currently accepting RTP)



Not shown: 5% selecting don't know / prefer not to say

↑ = Significantly higher vs. other segments ↓ = Significantly lower vs. other segments

© Visa 2026. All rights reserved.

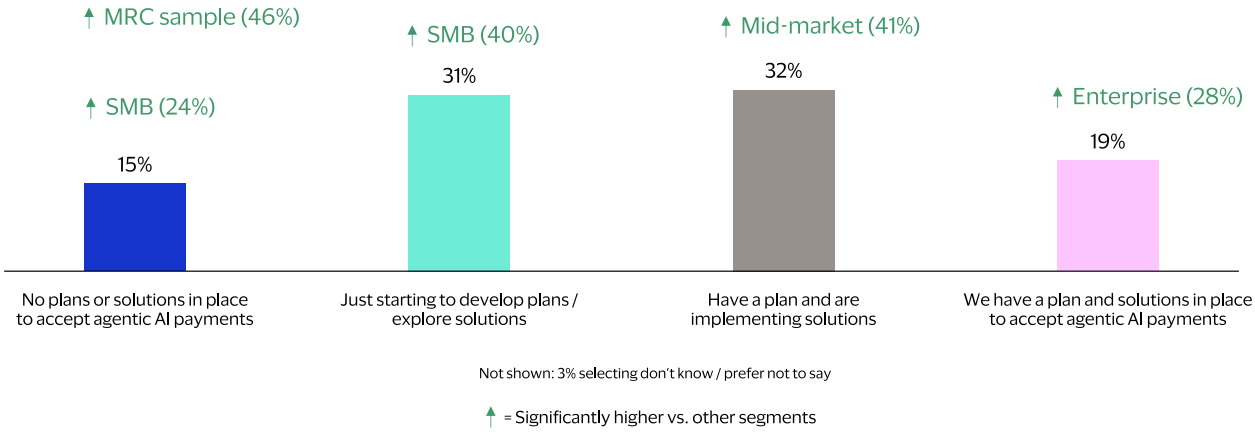
Section 1: Payment acceptance

While these data points underscore the strong momentum RTP has in the market as a new acceptance method, one important caveat to keep in mind is that RTP adoption will vary significantly in speed and scale for certain merchant segments. For instance, MRC members surveyed this year are significantly less likely to report RTP adoption (only 24% claim current acceptance, as shown in Figure 7). And MRC members also report significantly lower likelihood of adding this method over the next year compared with non-MRC enterprises (see Figure 9).

Agentic AI payments loom large on the horizon, with most merchants making plans for implementation

As merchants increasingly incorporate RTP into eCommerce acceptance offerings, many are also looking ahead to a near future in which payments can be made on humans' behalf by AI agents or assistants. When asked to describe their organization's current readiness to accept such "agentic AI" payments, almost one in five (19%) are currently set up to accept agentic AI payments now (see Figure 10). The majority (63%) are still in the midst of planning and implementation, with 32% in the early implementation stage, and another 31% in more of the planning and exploration phase. Only 15% say they have no plans or solutions in place to accept agentic AI payments anytime soon.

Figure 10: Readiness to accept agentic AI payments (2026, all payment professionals)



As with other payment methods, the rollout of agentic AI payments is being led by the largest merchants. Enterprise merchants in this year's survey are significantly more likely to say they have solutions in place, while mid-market merchants are more likely to be implementing solutions. Most SMBs are either planning or taking a more cautious approach. MRC members are far more likely than other merchant segments to be holding off on adopting agentic AI payments, with nearly half (46%) in this year's survey saying they have no plans or solutions in place (see Figure 10).

© Visa 2026. All rights reserved.

Section 2:

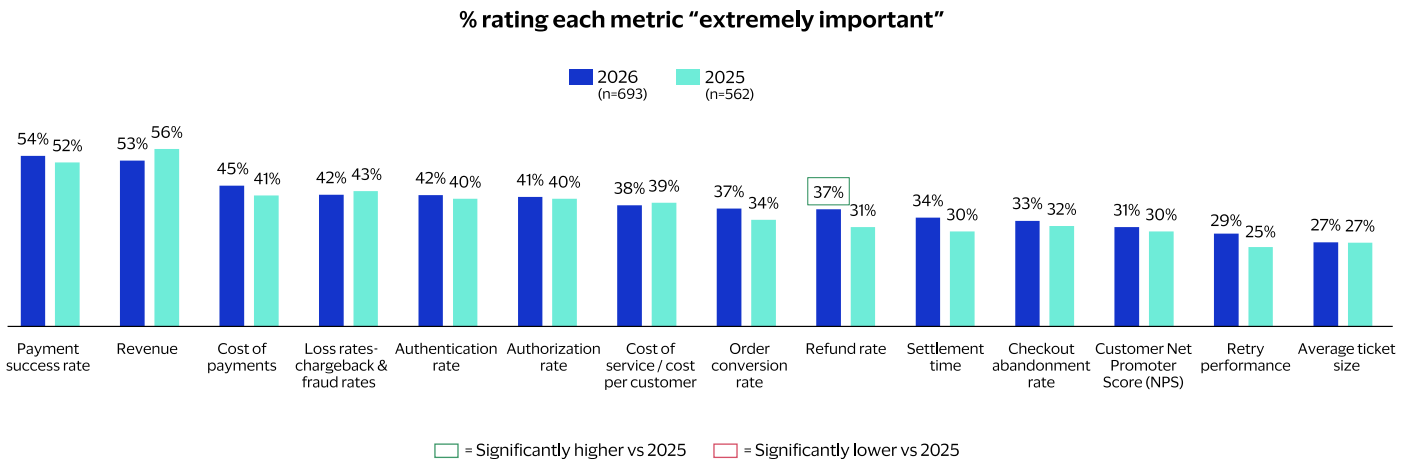
Payment metrics and tactics

In this section, the focus shifts from payment acceptance to payment metrics and tactics, specifically which metrics and performance indicators merchants consider most important to their business, as well as how they are using advanced tools such as payment tokenization to maximize efficiency, security, and customer satisfaction.

Merchants highlight payment success rate and revenue as the two most critical KPIs

Out of 14 payment metrics tested in this year's survey, two stand out as most important to merchant payment professionals: payment success rate* and revenue. Similar to last year, more than half of those surveyed this year rate these two metrics "extremely important," the highest importance option offered on a five-point scale in our survey (see Figure 11). The elevation of these two metrics compared to all others underscores the paramount importance merchants place on maximizing both efficiency and profitability in this part of the business.

Figure 11: Importance of payment metrics (2025-2026, all payment professionals)



*Note: "Payment success rate" is the share of payments that are successfully completed from "end-to-end," i.e., fully settled.

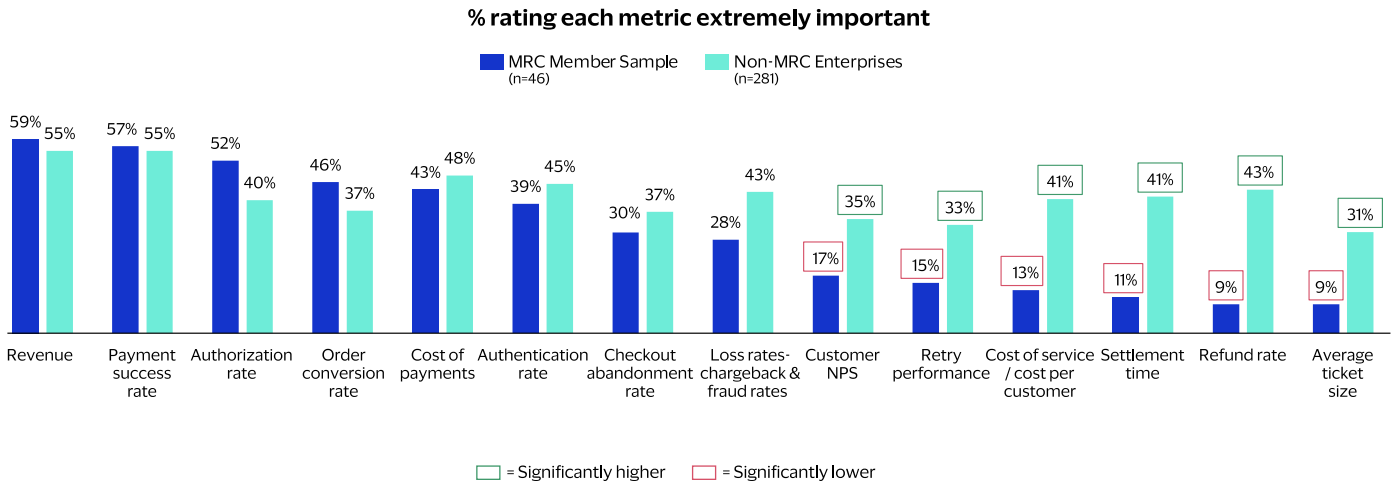
Beyond the top two KPIs, merchants point to a handful of others seen as "extremely important" by a sizable share (40-50%) in today's marketplace. These include cost of payments, loss rates (due to fraud & chargebacks), authentication rate, and authorization rate. Again, the common thread between these secondary KPIs is that they all primarily measure the efficiency or profitability of payment offerings and operations (although loss rates also incorporate some indirect assessment of customer satisfaction, tied to chargebacks, and payment security, reflected in fraud rates).

© Visa 2026. All rights reserved.

Section 2: Payment metrics and tactics

The survey data shows a prominent difference in the views of MRC members and non-MRC enterprises on the importance of various metrics, as illustrated by the data in Figure 12. While there are some directional differences in these figures for a few of the most important metrics (e.g., 52% of MRC members giving authorization rate the highest importance rating, versus 40% of non-MRC enterprises), the two groups generally share similar views on the importance of the first eight metrics on the left side of the chart. Where their views diverge is on the six metrics on the right side of the chart: MRC members are far less likely to consider customer Net Promoter Score, retry performance, cost of service, settlement time, refund rate, and average ticket size as important payment KPIs compared with non-MRC enterprises.

Figure 12: Importance of payment metrics, by MRC membership (2025–2026, payment professionals)



These data, which have exhibited a consistently similar pattern for several consecutive years in this study, may indicate that MRC members are successfully honing in on a short list of signals they see as most meaningful, while placing less emphasis on other indicators. Conversely, non-MRC enterprises appear more apt to take a more exhaustive approach to tracking payment metrics, keeping tabs on a larger basket of KPIs pertaining to their eCommerce payment programs over time.

© Visa 2026. All rights reserved.

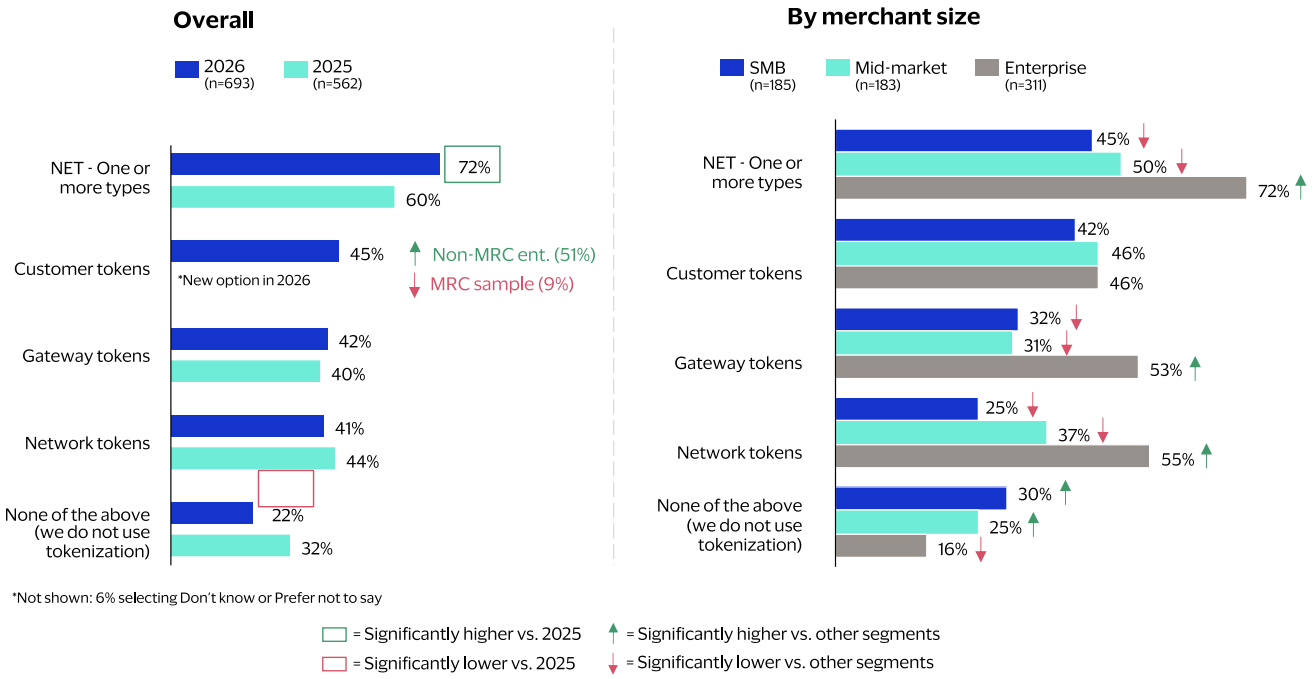
Section 2: Payment metrics and tactics

Payment tokenization continues as a common practice, especially among enterprises

More than seven in ten merchants (72%) say they use one or more forms of payment tokenization, representing a significant year-on-year increase of 12% (see Figure 13). This increase is partly driven, however, by the addition of customer tokens * as a new option in this year's survey, joining gateway and network tokens.

*Note: Customer tokens are merchant-created identifiers tied to customer profiles, used across channels for personalization and saved-payment experiences.

Figure 13: Use of payment tokenization, overall and by merchant size (2025–2026, all payment professionals)



Overall, the data show similar usage rates for all three forms of tokenization, with 40–45% of merchants currently using each. But the data also shows a distinct disparity in use of customer tokens, specifically between MRC members and non-MRC enterprises: more than half of the latter group (51%) currently use customer tokens, compared with just 9% of MRC members.

Another recurring pattern replicated in this year's data is the strong association between merchant size and use of tokenization, as depicted by the right-hand chart in Figure 13. Enterprise merchants are significantly more likely than mid-market and SMB merchants to use both gateway and network tokens. Overall, this means that more than seven in ten enterprise merchants use some form of payment tokenization, versus just 50% of mid-market merchants and 45% of SMBs.

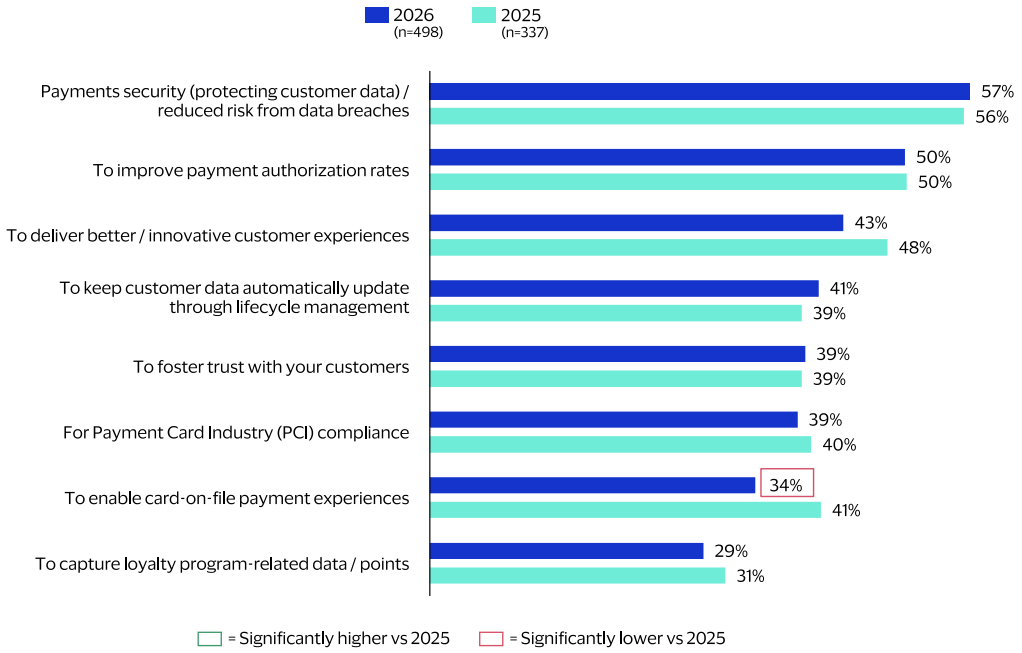
© Visa 2026. All rights reserved.

Section 2: Payment metrics and tactics

Protecting customer data and reducing risk from data breaches remain the top reasons for using tokenization

Merchants cite multiple reasons for utilizing payment tokens, with enhanced payment security/data protection first and foremost, followed by improved authorization rates, both cited by at least 50% in this year's survey (see Figure 14). Other motivations cited by at least one-third of token users in this year's survey include delivering stronger customer experiences, bolstering trust among customers, and complying with Payment Card Industry Data Security Standards (PCI DSS).

Figure 14: Reasons for using payment tokenization (2025–2026, all payment professionals using tokenization)



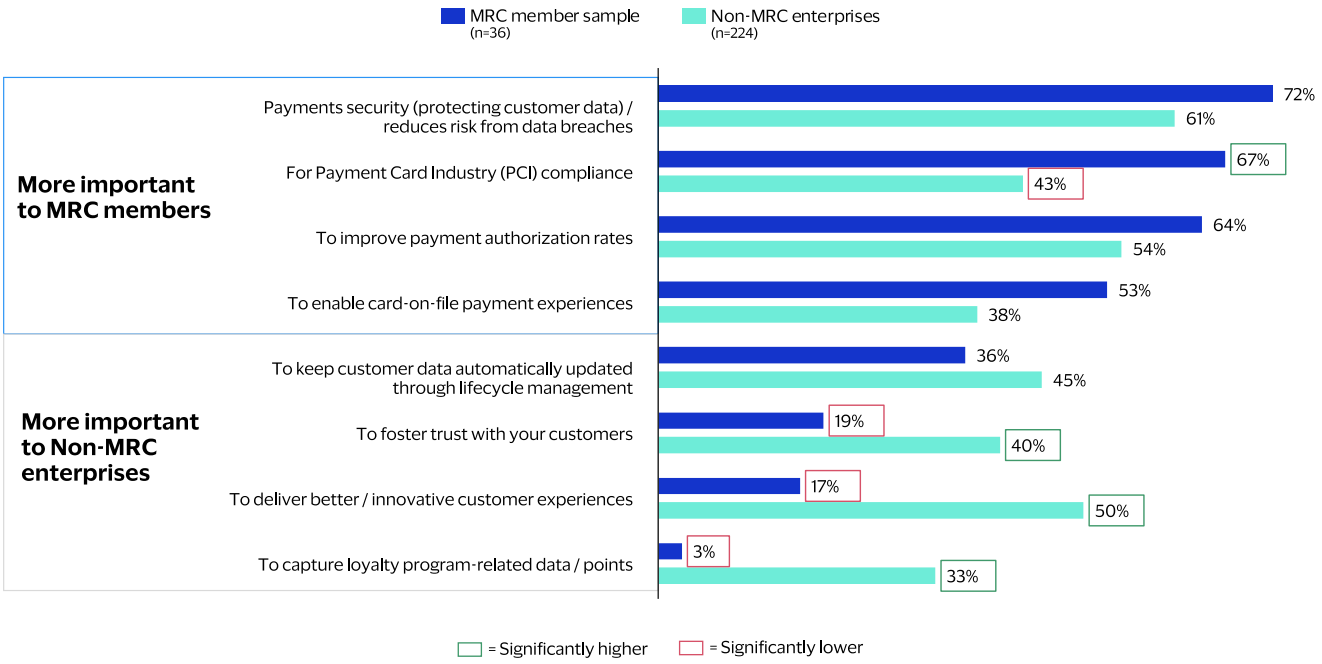
While merchants' motivations for deploying tokens generally stay consistent over time, there was one significant change in the data collected this year: The share of merchants citing enablement of card-on-file payment experiences as a reason for using tokens declined significantly, falling to 34% this year from 41% last year. There was also a directional decrease in the share citing "delivery of better/innovative customer experiences" as a motivating factor (from 48% last year to 43% this year). These data may indicate a lessened focus on customer outcomes among merchants using payment tokens, although more research is needed to establish conclusively whether this will be a significant, persistent change in how and why merchants use payment tokenization.

© Visa 2026. All rights reserved.

Section 2: Payment metrics and tactics

One trend that is well-established as a consistent pattern is a difference in why MRC members use tokenization versus non-MRC enterprises. As shown in Figure 15, MRC members are more likely to say they use tokenization for increased payments security, greater assurance of PCI DSS compliance, and enablement of card-on-file experiences. While many non-MRC enterprises also indicate these factors as important, they are significantly more likely to cite a few other reasons, as well, including delivering better customer experiences, fostering trust with customers, and capturing loyalty program-related data.

Figure 15: Reasons for using tokenization, by MRC membership (2026, payments professionals using tokenization)



Merchants employ multiple tactics to improve authorization rates while enhancing security and CX

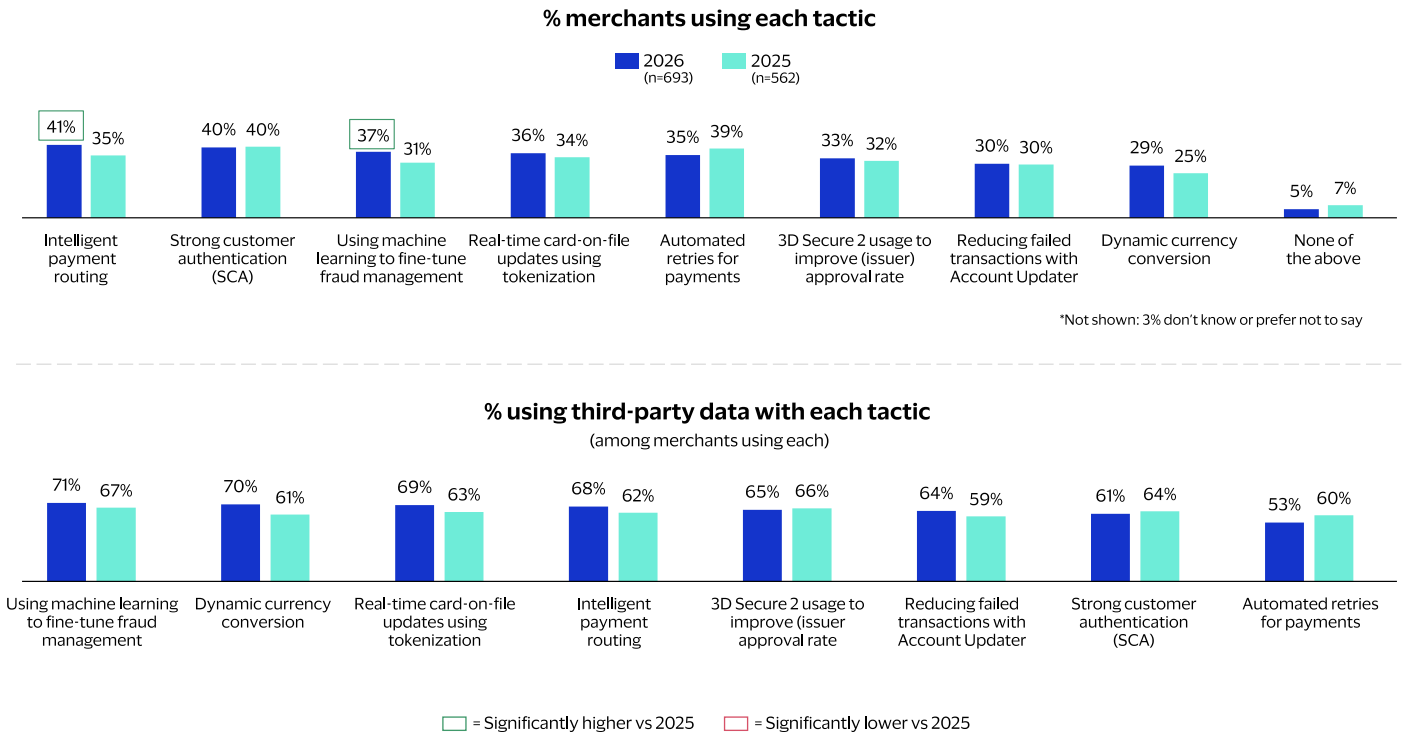
In addition to payment tokenization, merchants employ an array of other advanced tools and tactics to improve authorization rates, strengthen security, and support strong customer experiences. As shown by the top chart in Figure 16, intelligent payment routing and strong customer authentication (SCA) are the most popular, with four in ten indicating they currently use each.

© Visa 2026. All rights reserved.

Section 2: Payment metrics and tactics

Several other tactics are widely used, as well, including fraud management tools fine-tuned with machine learning (ML), real-time card-on-file updates, automated retries, and 3D Secure 2 (3DS2). And as illustrated by the bottom chart in Figure 16, third-party data is instrumental to the effectiveness of these tools to enhance risk assessment, reduce fraud and false positives, and improve the user experience. Most merchants are using third-party data across various authentication methods, with 70% using third-party data to support ML fine tuning of fraud tools and dynamic currency conversion.

Figure 16: Use of authorization-related tactics and supporting third-party data (2025-2026, all payment professionals)



© Visa 2026. All rights reserved.

Section 3:

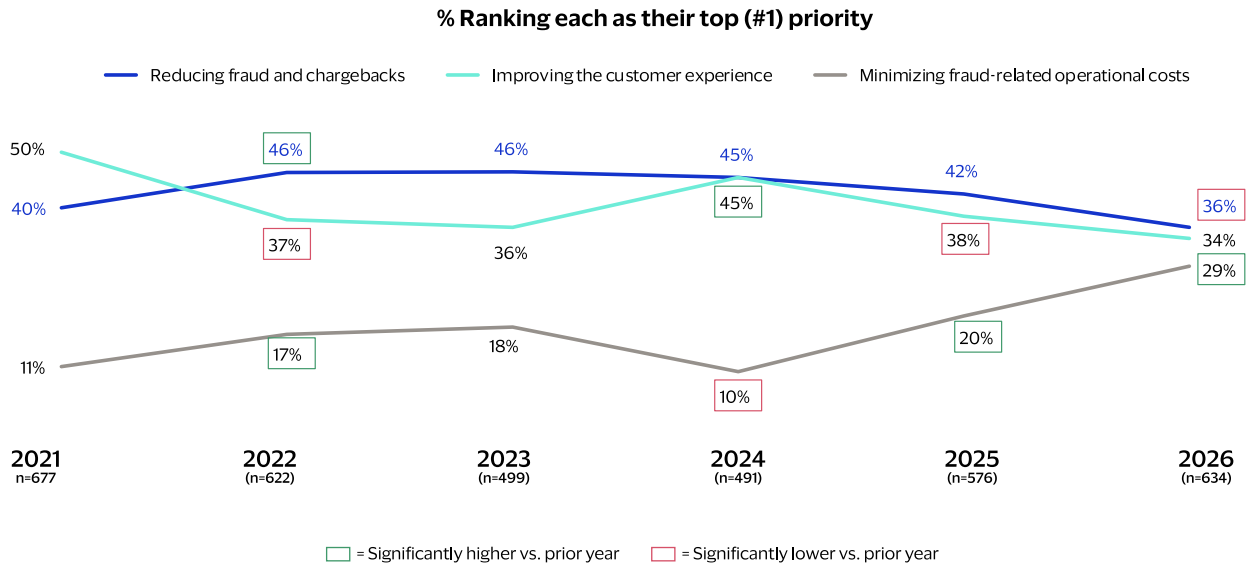
Fraud management strategies and challenges

The next three sections of this report offer fresh insights about topics and trends in eCommerce fraud. This section starts at a high level, shedding light on merchants' top goals and challenges in fraud management today and how those are influencing their future strategies and spending plans.

Cost concerns keep mounting, spurring merchants to prioritize profitability and pull back on spending

Each year, merchant fraud professionals rank their top strategic priority between reducing fraud and chargebacks, improving the customer experience, or minimizing operational costs. For the past several years, merchants invariably prioritized the first two goals over the latter, usually by a wide margin. But since 2024, these data have shown a steady, significant shift in strategic priorities: More and more merchants are citing cost minimization as their number one goal, while fewer and fewer are keeping the focus primarily on reducing fraud or on improving CX. In fact, for the first time ever in our research, all three objectives now have statistically equivalent shares of merchants ranking them as the top priority (see Figure 17).

Figure 17: Top fraud management priority (2021–2026, fraud professionals)

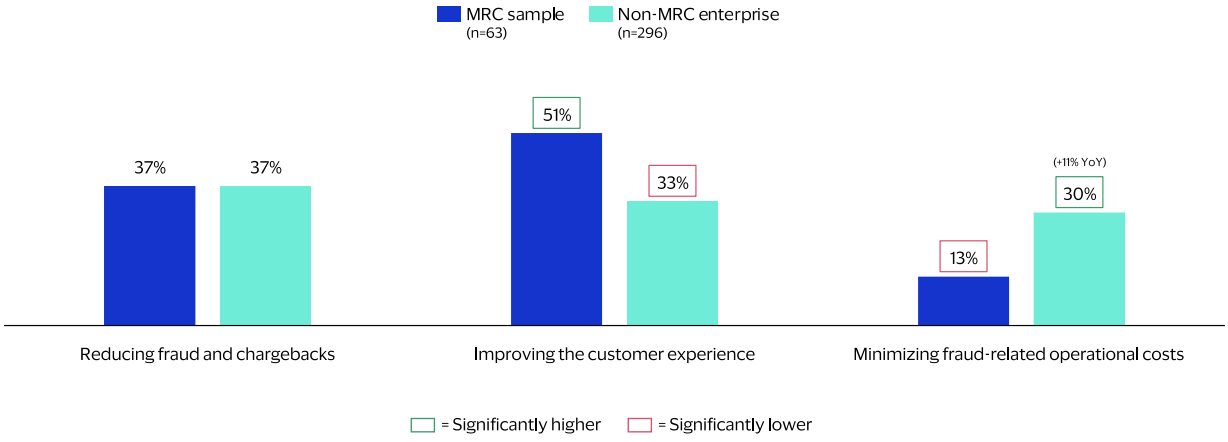


Clearly, this data shows cost concerns are mounting quickly for merchant fraud professionals. But it also illustrates how this "belt tightening" imperative effectively heightens tensions and forces trade-offs on other fundamental fraud management priorities. In other words, merchants are facing more pressure than ever to check off not just one or two of these strategic boxes but to accomplish all three at the same time.

© Visa 2026. All rights reserved.

Section 3: Fraud management strategies and challenges

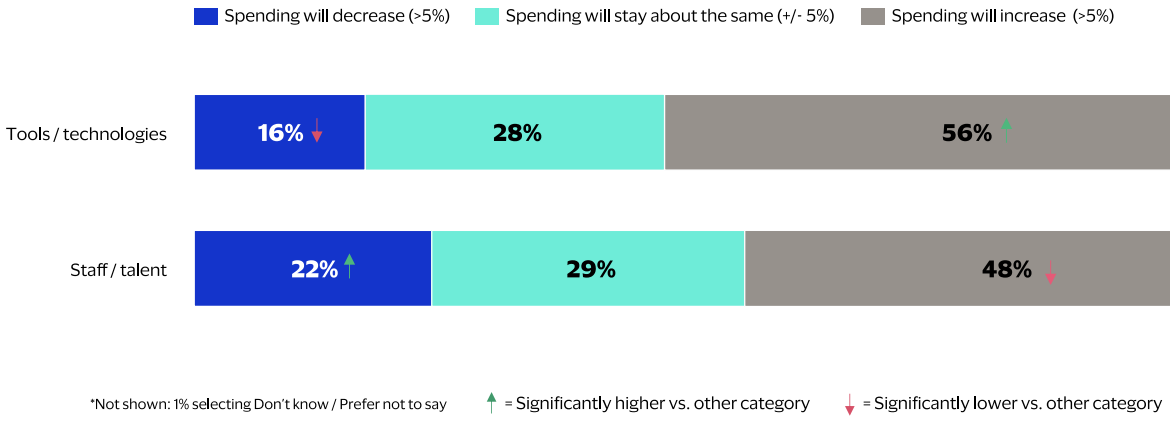
Figure 18: Top fraud management priority (2026), by MRC membership



It is important to point out that this picture of conflicting priorities looks much different for MRC members. The majority of MRC merchants (51%) are still focused primarily on improving customer experience and second on reducing fraud and chargebacks (see Figure 17). Only 13% cite minimizing costs as their top priority, in contrast to 30% of non-MRC enterprises.

Growing cost concerns are evident in other survey data this year as well. When asked about future investments, the majority (52%) say they expect spending on fraud management staff/talent to stay flat or decrease over the next two years, and 44% project flat or decreased spending on tools and technologies in this area (see Figure 19).

Figure 19: Expected changes in fraud management spending over next two years (senior fraud professionals)



While this means 56% are still projecting higher spending on tools and tech in the near term, it represents a decrease of 7 percentage points from the 63% who said this in last year's survey. Altogether, these data points paint a stark picture of fraud management professionals being challenged to "do more with less," in this area of merchants' business.

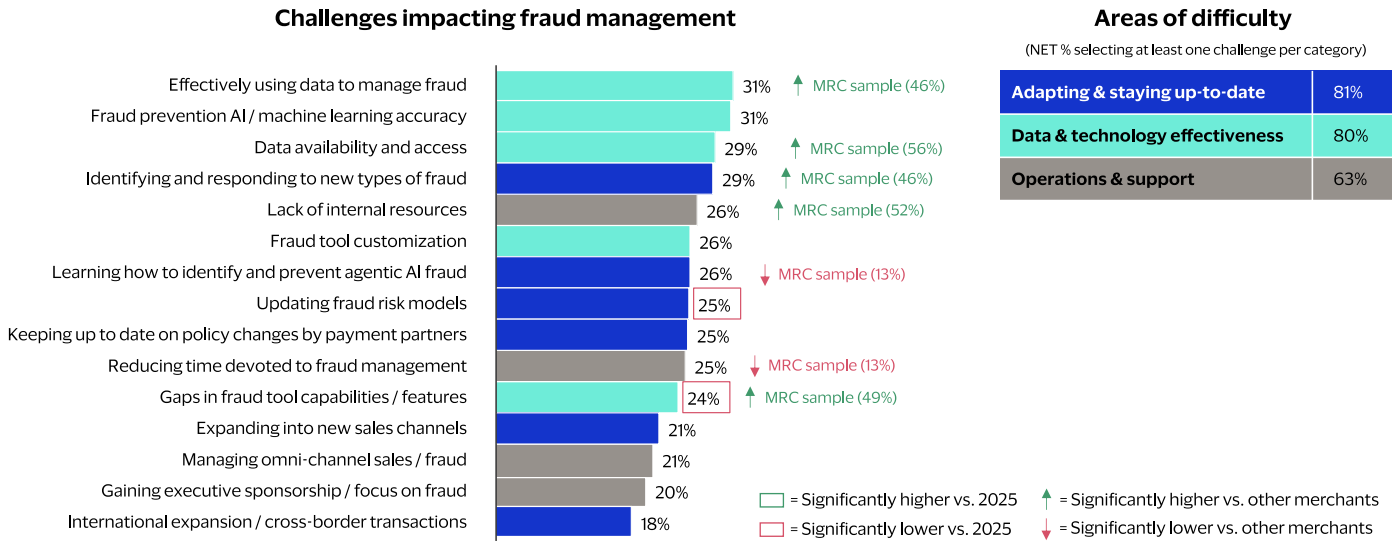
© Visa 2026. All rights reserved.

Section 3: Fraud management strategies and challenges

Data and technology is a major source of frustration and the main area for improvement in 2026

While cost constraints pose challenges, the biggest source of frustration for merchant fraud professionals is data and technology. When presented with 15 different challenges, merchants in this year's survey cited data and technology-related issues as four of the top six, overall (see Figure 20). These include effectively using data to manage fraud, the accuracy of AI/ML fraud tools, the availability and access to relevant data, and fraud tool customization. All four are cited by at least one-quarter of merchants in this year's survey, and in total, 80% say they are struggling with at least one of the five data and tech-related issues in the survey.

Figure 20: Fraud management challenges (2026, fraud professionals)

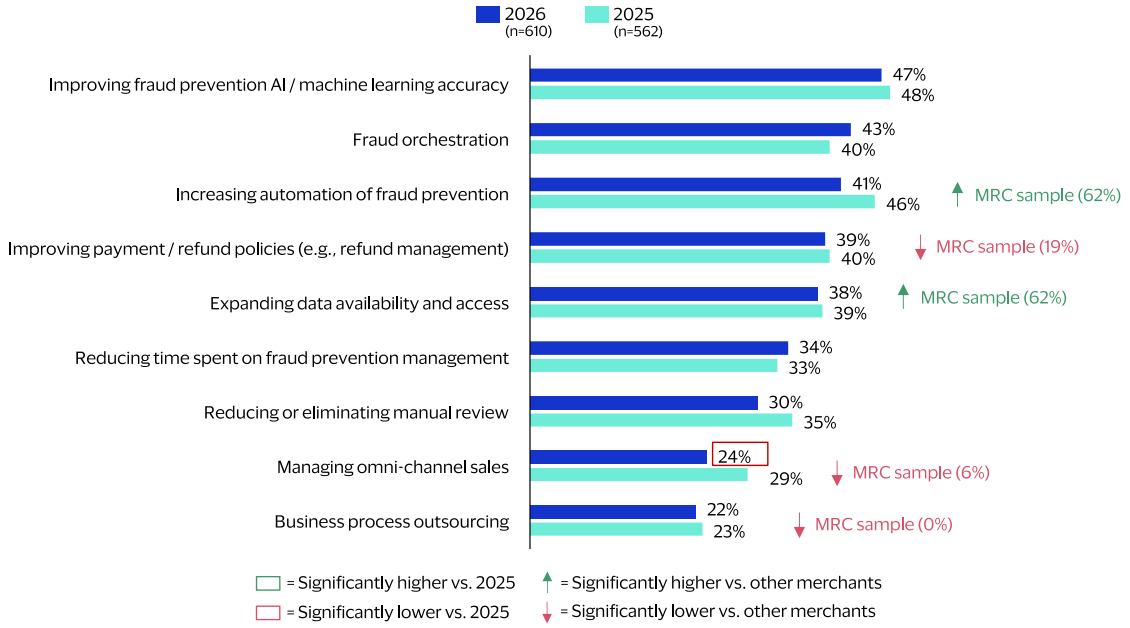


Data and technology issues are especially vexing for MRC members, as indicated by the significant difference callouts in Figure 20. MRC members are far more likely to cite availability and access, as well as effective use of, data for anti-fraud purposes as a key challenge. And roughly half (49%) cite gaps in fraud tool capabilities and features, versus just 24% of merchants overall. MRC members are also significantly more likely to struggle with two other top challenges: identifying and responding to new types of fraud and lack of internal resources.

© Visa 2026. All rights reserved.

Section 3: Fraud management strategies and challenges

Figure 21: Top improvement areas over the next 12 months (2025-2026, fraud professionals)

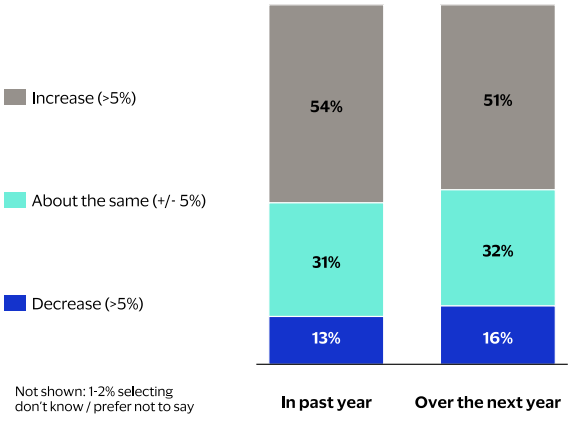


With data and technology sitting front and center in terms of fraud management challenges, it is no surprise that merchants' top improvement areas for 2026 are anchored in this area as well. Figure 21 shows a snapshot of the improvement areas cited by merchants over the past two years. Four of the top five areas relate directly to data and tech: improving accuracy of AI/ML fraud tools, fraud orchestration, increasing automation of fraud prevention, and expanding data availability and access. Each of these is a priority for roughly 40-50% of merchants, globally, and the latter two (increasing automation and data availability) are significantly more important to MRC members (62%).

Facing increasing budget pressures and several frustrating kinks in the tech stack, merchant fraud professionals are no doubt placing more a premium on efficiency, not just in terms of financial costs but also time and labor. More than half (52%) say they have been spending more and more time on fraud prevention management over the past year, and most (51%) expect that to continue in 2026 (see Figure 22). This contrasts starkly with the mere 13% who say they've been able to save time in this area over the past year and 16% who expect to spend less time on this over the next.

With most merchants projecting flat or decreased spending on fraud management staff and talent in the near future (see Figure 19), fraud professionals will no doubt need to use their time more efficiently and effectively in order to "do more with less" moving forward.

Figure 22: Trends in time spent working on fraud prevention management (2026, fraud professionals)



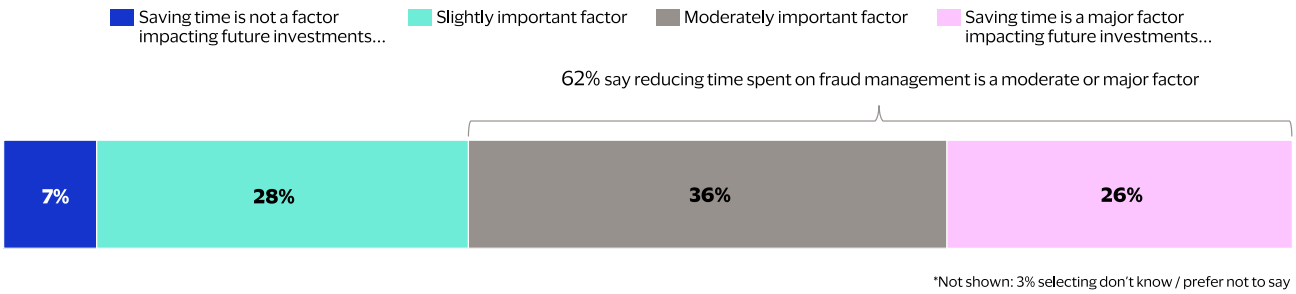
© Visa 2026. All rights reserved.

Section 3: Fraud management strategies and challenges

This helps explain why a clear majority (62%) say the ability to reduce or minimize time spent on fraud management will be an important factor in their investment decisions over the next one to two years (see Figure 23). And even among those who do not view time savings as a major driver of future investments, there are very few (7%) who say it will have no impact at all on their future investments in this area.

Overall, this year's survey shows increasing pressure for merchants in the area of fraud management due to mounting financial pressures, data and technology challenges, and increasing demands for time and labor.

Figure 23: Importance of time savings in fraud management investments over next two years (2026, fraud professionals)



*Not shown: 3% selecting don't know / prefer not to say

© Visa 2026. All rights reserved.

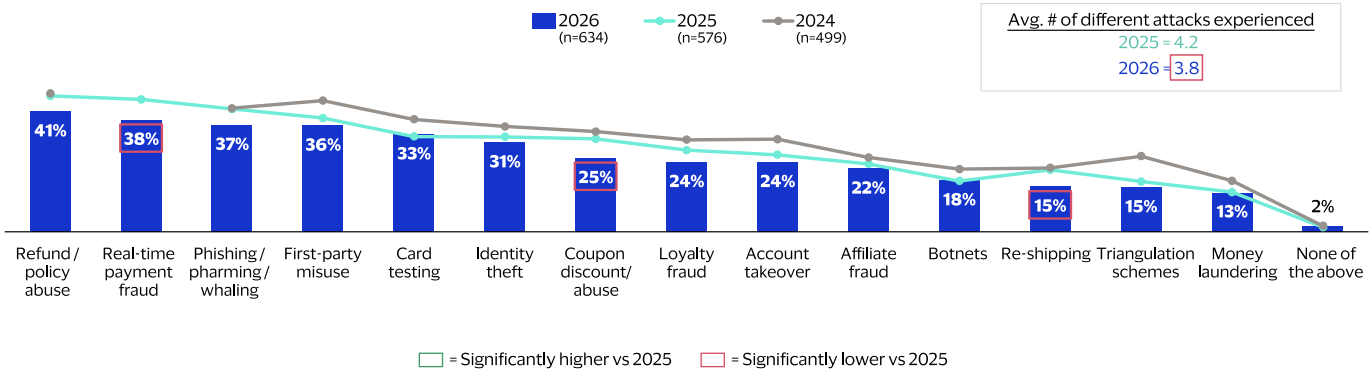
Section 4:

Fraud management metrics and tactics

This section drills down beyond the high-level strategies and challenges impacting merchant fraud professionals, providing quantitative benchmarks for key fraud management metrics, shedding light on the tactics merchants are using to identify and prevent fraud, and gauging merchant use of advanced anti-fraud tools.

Incidence rates of fraud decline for a second consecutive year, including significant declines for some attacks
Fraud remains a universal challenge for merchants, with 98% reporting at least one form of fraud attack over the past 12 months (a figure that has stayed consistent over several years of this research). But for the second consecutive year, our data show across-the-board declines in the share of merchants experiencing the 14 specific types of fraud covered in the survey (see Figure 24). The average number of different attacks experienced by merchants in this year's survey declined significantly, falling from 4.2 last year to 3.8 this year.

Figure 24: Types of fraud experienced in past 12 months (2024–2026, fraud professionals)



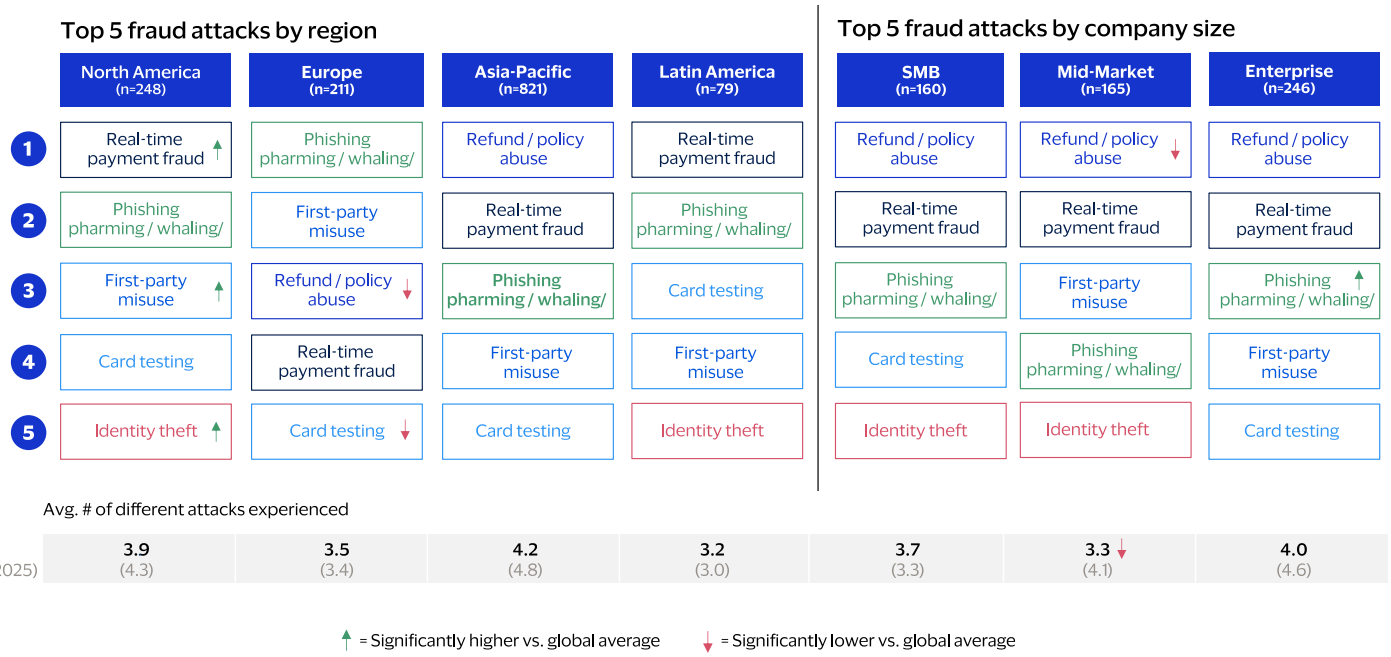
Still, the top five most common forms of fraud continue to impact at least one-third of merchants globally: refund/policy abuse, real-time payment fraud, phishing/pharming/whaling, first-party misuse, and card testing. Merchants may be making progress in tamping down RTP fraud, as this is one of three fraud attacks showing a significant decrease in reported incidence versus last year (from 45% to 38%). The other two are coupon/discount abuse, which decreased from 32% to 25%, and re-shipping, which dropped from 22% to 15%.

© Visa 2026. All rights reserved.

Section 4: Fraud management metrics and tactics

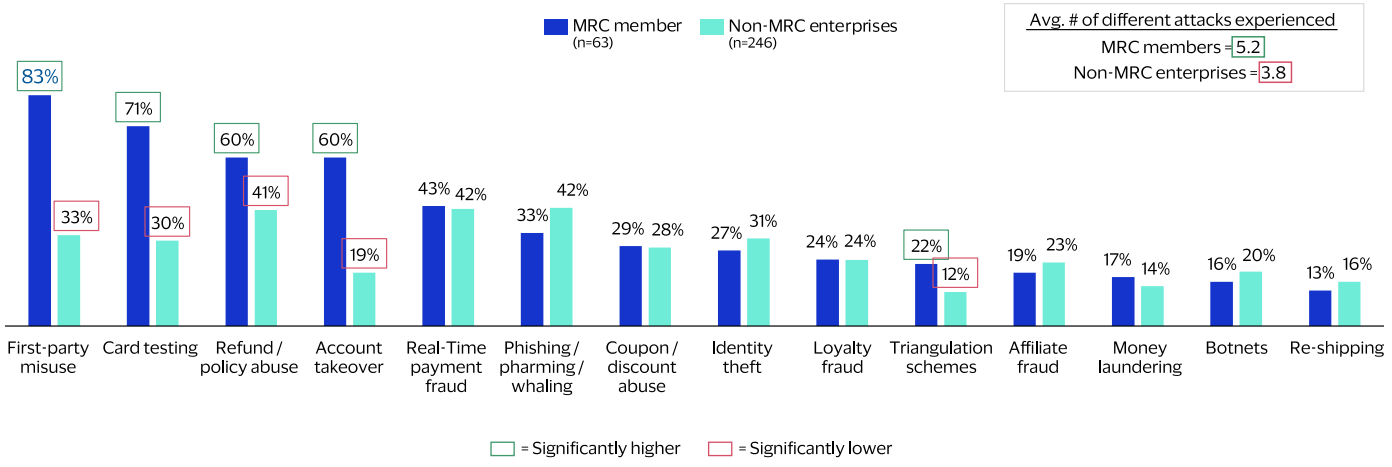
Figure 25 displays the top fraud attacks for merchants in each geographic region and size tier. Those in North America over-index on reported incidence of RTP fraud, first-party misuse, and identity theft, while those in Europe report significantly lower rates of refund/policy abuse and card testing attacks compared with the global average. Enterprise merchants are more likely than others to experience phishing/pharming/whaling fraud. Mid-market merchants report significantly lower incidence of refund/policy abuse, as well as significantly fewer different fraud attacks on average than globally.

Figure 25: Top five fraud attacks experienced in past 12 months, by region and size segment (2026, fraud professionals)



As in previous years, MRC members report experiencing a greater variety and volume of fraud attacks compared with non-MRC enterprises (see Figure 26). MRC merchants experienced 5.2 attacks in the past year, on average, compared with 3.8 for non-MRC enterprises. When it comes to specific types of fraud, MRC members are significantly more likely to report first-party misuse, card testing, refund/policy abuse, account takeover, and triangulation scheme attacks.

Figure 26: Fraud attacks experienced in past 12 months, by MRC membership (2026, fraud professionals)



© Visa 2026. All rights reserved.

Section 4: Fraud management metrics and tactics

It is important to point out that these differences in fraud incidence between MRC members and non-MRC enterprises are due to a combination of factors: First, MRC members likely do face a wider variety and higher volume of fraud attacks than non-member enterprises each year, and second, MRC members are also more likely than non-members to be monitoring for fraud, especially at the point of purchase and payment/checkout (see Figure 30). Therefore, MRC members may be reporting higher incidence for certain forms of fraud because they are better able to detect and register such attempts in the first place.

Other fraud-related metrics generally stay consistent compared with last year

While the continued declines in fraud incidence rates are encouraging, other fraud-related metrics changed little, with most showing minor directional shifts up or down compared with last year. These metrics are summarized in Figure 27, both at the overall level and by region, size, and MRC membership. Average fraud rate by order is the one metric that did show a significant change at the overall level, increasing from 3.0% in 2025 to 3.5% this year.

Figure 27: Fraud-related metrics (2025–2026, fraud professionals)

Fraud-related metrics (trimmed averages shown)	2025	2026	Region				Size			MRC membership	
			North America	Europe	Asia-Pacific	Latin America	SMB	Mid-market	Enterprise	MRC sample	Non-MRC enterprises
Fraud rate by revenue (% of total annual eCommerce revenue lost to payment fraud globally)	3.2%	3.5%	3.1% (3.6)	4.1% (2.8)	3.0% (2.6)	4.1% (4.1*)	3.4% (3.4)	4.5% (3.2)	3.2% (3.3)	0.6% (0.5)	3.9% (4.4)
Fraud rate by order (% accepted orders in past 12 months that turned out to be fraudulent)	3.0%	3.5%	3.4% (3.4)	3.8% (2.8)	3.0% (2.5)	3.5% (3.9)	3.3% (3.4)	4.0% (3.0)	3.4% (3.1)	0.3% (0.4)	4.0% (4.0)
Order rejection rate (% eCommerce orders rejected due to suspicion of fraud in past 12 months)	5.0%	5.2%	4.6% (5.2)	5.7% (5.2)	5.9% (4.5)	5.4% (5.9)	5.1% (5.0)	6.0% (4.6)	4.9% (5.4)	2.8% (2.5)	5.2% (6.2)
Chargeback / dispute win rate (annual % of fraud-coded chargebacks & disputes won by the)	17.1%	16.7%	19.8% (17.9)	15.3% (15.1)	16.2% (19.6)	12.2% (11.5)	18.5% (18.2)	15.9% (17.0)	15.8% (16.4)	27.4% (27.1)	14.5% (15.0)

= Significantly higher vs. other segments = Significantly lower vs. other segments (% = 2025 figures)

There are significant differences in these indicators for merchants in different regions and size tiers. Those in North America claim a significantly higher chargeback/dispute win rate, as well as a significantly lower order rejection rate, versus those in other regions (see Figure 27). Latin American merchants claim a significantly lower chargeback/dispute win rate than others. Mid-market merchants report higher fraud rates by revenue, as well as higher order rejection rates, versus SMBs and enterprises.

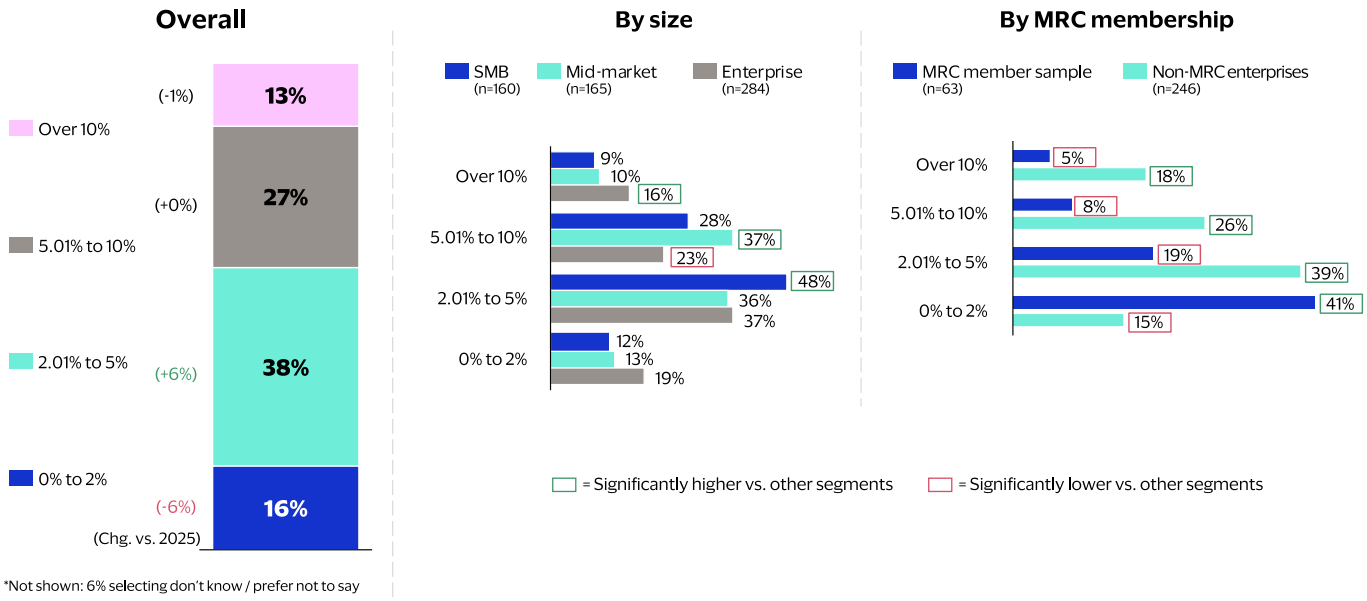
And consistent with a long-running trend in our research, the fraud-related metrics reported by MRC members are significantly better than those claimed by non-MRC enterprises. Average fraud rate by revenue, fraud rate by order, and order rejection rate are all significantly lower for MRC merchants, while their estimated win rate for chargebacks and disputes is two times higher than the win rate reported by non-MRC enterprises (see Figure 27). While MRC members may face more fraud each year, these figures continue to show they have far greater success than non-member enterprises when it comes to preventing fraud and mitigating its harmful impacts on their organizations and customers.

© Visa 2026. All rights reserved.

Section 4: Fraud management metrics and tactics

In addition to the impacts quantified by the metrics in Figure 27, eCommerce fraud also takes a toll on merchants' relationships with both individual customers and payment partners. One indicator of this is the number of "customer insults," or false positives, that merchants experience when they dispute legitimate orders they believe to be fraudulent. Figure 28 shows that roughly two-thirds of merchants (65%) currently estimate their rate of false positives on eCommerce orders somewhere between 2% and 10%, with the majority of this group giving estimates on the lower end of this range.

Figure 28: Rate of false positives or "customer insults" (2025-2026, fraud professionals)



This year's survey shows a significantly larger share of merchants citing estimates between 2% and 5%, along with a significantly lower share citing estimates at 2% or less. Overall, this may indicate rising numbers of customer insults occurring in the marketplace, something merchants should keep a close eye on in the coming year to avoid doing undue damage to their relationships with customers and payment partners.

Also depicted in Figure 28 are two bar charts showing how false positive rates vary by size and MRC membership. At a high level, the average rate of false positives tends to increase along with merchant size, although there is a bit of nuance to this, as enterprises are not only more likely to report rates exceeding 10% but also more likely to report rates below 2% compared with smaller merchants. MRC members outperform non-MRC enterprises by a considerable margin in this area as well. More than four in ten MRC merchants (41%) report false positive rates less than 2%, while more than four in ten non-MRC enterprises (44%) report rates higher than 5%.

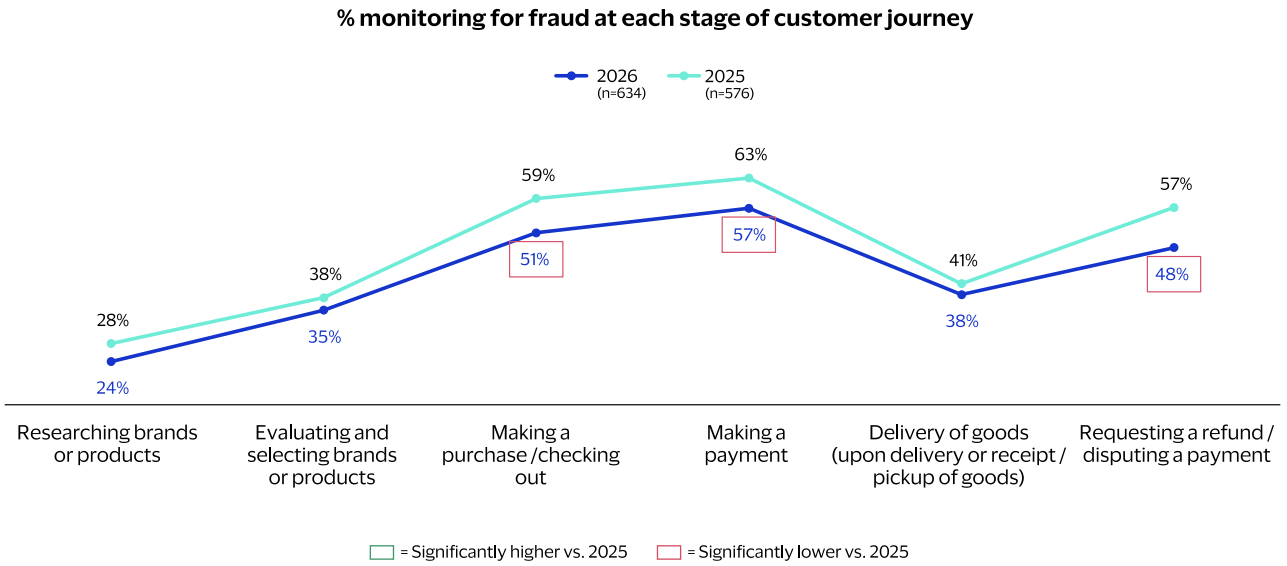
© Visa 2026. All rights reserved.

Section 4: Fraud management metrics and tactics

Usage rates decline slightly for many advanced fraud prevention tactics and tools

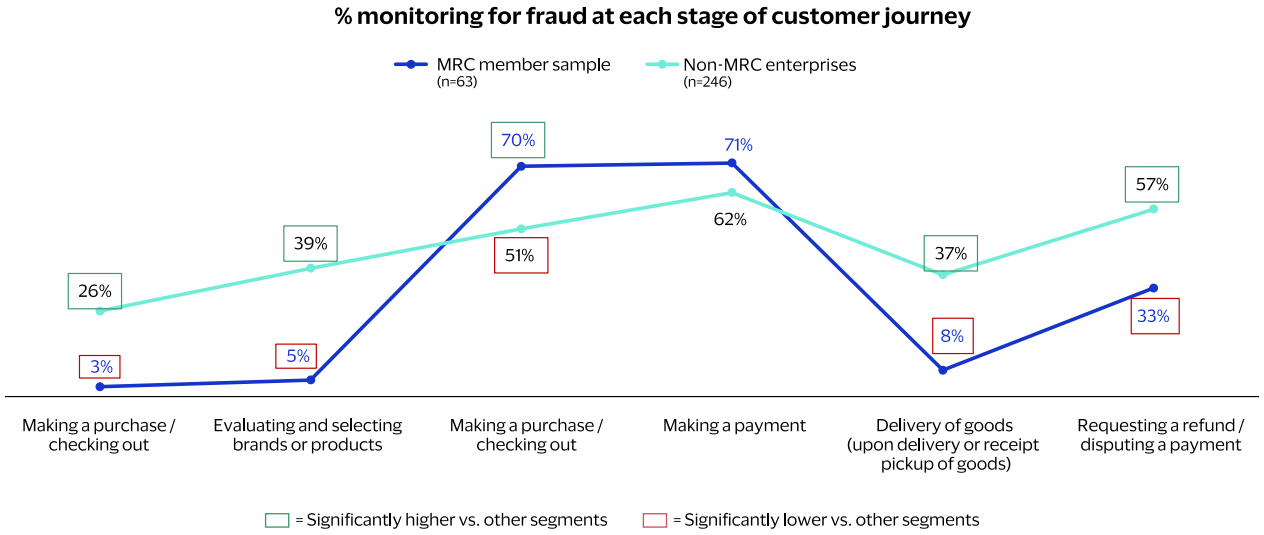
Turning from the metrics that merchants use to assess fraud rates and impacts to the specific means by which they combat fraud, this year's survey generally shows decreases in the shares of merchants using many of the advanced fraud prevention tactics and tools available in the market. For instance, the shares of merchants claiming they monitor for fraud at each stage of the consumer journey have all fallen, year-over-year, as depicted by the chart in Figure 29.

Figure 29: Fraud monitoring throughout the customer journey (2025–2026, fraud professionals)



These declines are statistically significant for fraud monitoring at key stages of the journey: the point of purchase (or checkout), the point of payment, and post-purchase, when customers request a refund or initiate a dispute.

Figure 30: Fraud monitoring throughout the customer journey, by MRC membership (2026, fraud professionals)



Here again, MRC members take a different tack than non-MRC enterprises, as illustrated by the chart in Figure 30. The latter are significantly more likely to report fraud monitoring at all the pre-purchase and post-purchase stages shown in

© Visa 2026. All rights reserved.

the survey, while the former are significantly more likely to monitor for fraud at the point of purchase, or checkout, and also directionally more likely to do so at the point of payment.

While there may be some pullback among merchants in the use of fraud screening tools throughout the customer journey, survey data show they are continuing to shift away from manual screening of eCommerce orders and toward digital screening, slowly but surely. In 2024, the share of merchants screening orders manually was 25% globally. That figure has declined slowly but significantly over the past years, now sitting at 21% (see Figure 31). The average percentage of manually screened orders that are subsequently declined remains consistent with past years, now sitting at 18%. Over the same period that the share of orders screened manually has significantly decreased, the survey data has captured a similar, steady uptick in the share of orders screened digitally, from 51% in 2024 to 54% this year.

Figure 31: Digital versus manual order screening (2025–2026, fraud professionals)

	2025	2026	Region				Size			MRC membership	
			North America	Europe	Asia Pacific	Latin America	SMB	Mid-market	Enterprise	MRC sample	Non-MRC enterprises
Base	524	564	245	77	139	57	127	144	242	52	203
Avg. % of orders screened digitally (via software or other technologies)	52%	54%	55% (54%)	51% (53%)	55% (50%)	48% (41%)	56% (50%)	43% (52%)	56% (51%)	83% (86%)	52% (44%)
avg. % of orders screened manually (via human analysis or judgment)	23%	21%	22% (25%)	20% (21%)	26% (24%)	20% (21%)	21% (27%)	24% (24%)	20% (22%)	8% (3%)	22% (26%)
Avg. % of manually screened orders That are subsequently declined	19%	18%	18% (20%)	18% (16%)	13% (19%)	14% (16%)	18% (16%)	14% (19%)	18% (20%)	22% (23%)	17% (20%)

*Not shown: 5% selecting do not know / prefer not to say

= Significantly higher vs. other segments = Significantly lower vs. other segments

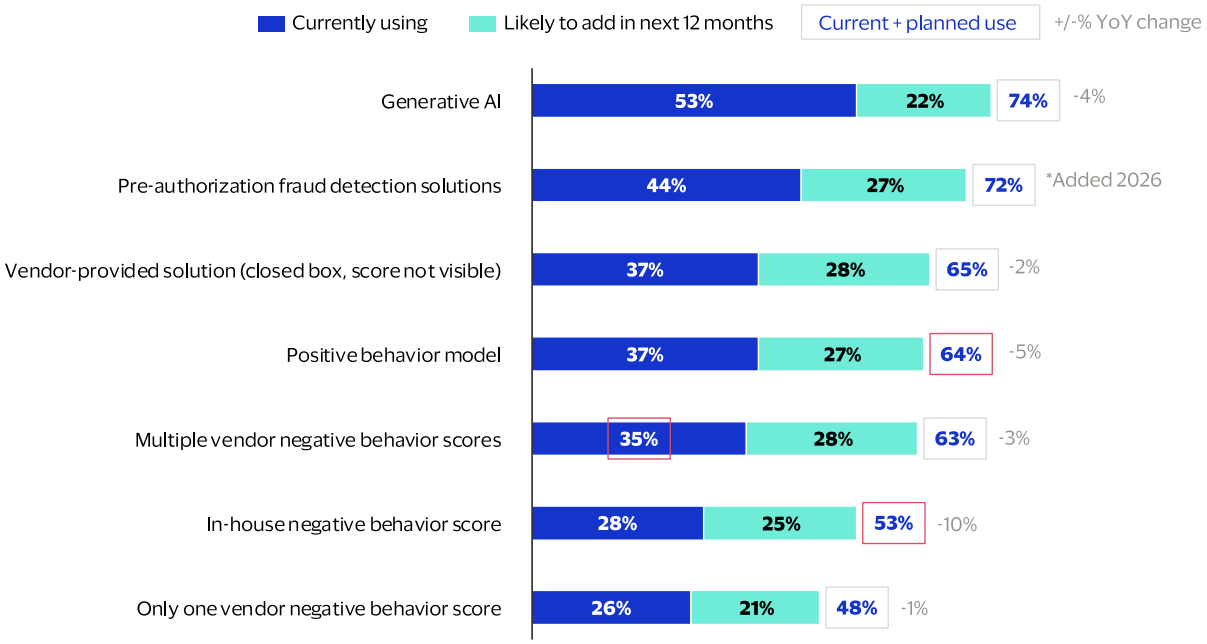
It is worth noting that mid-market merchants report screening a significantly smaller share of orders digitally, only 43% on average, versus the 56% reported by both SMBs and enterprises. This may help explain their higher fraud rate by revenue and/or the smaller number of different fraud attacks they report experiencing in the past year (see Figure 27 and Figure 25, respectively). By contrast, MRC merchants digitally screen a very high share of eCommerce orders: 83% on average, compared with the 52% reported by non-MRC enterprises. Of course, this also leads MRC members to screen significantly fewer orders manually as well.

© Visa 2026. All rights reserved.

Section 4: Fraud management metrics and tactics

The final set of insights in this section focuses on merchants' use of AI- and ML-powered fraud management tools. Here, the survey data again depict merchants pulling back a bit in terms of how many are using each of the tools displayed in Figure 32. While the changes have been directional in most cases, the data do show significant declines in the share of merchants currently using or planning to use positive behavior models and in-house negative behavior scores, as well as the share currently using multiple-vendor negative behavior scores.

Figure 32: Current and planned use of AI/ML fraud management tools (2026, fraud professionals)



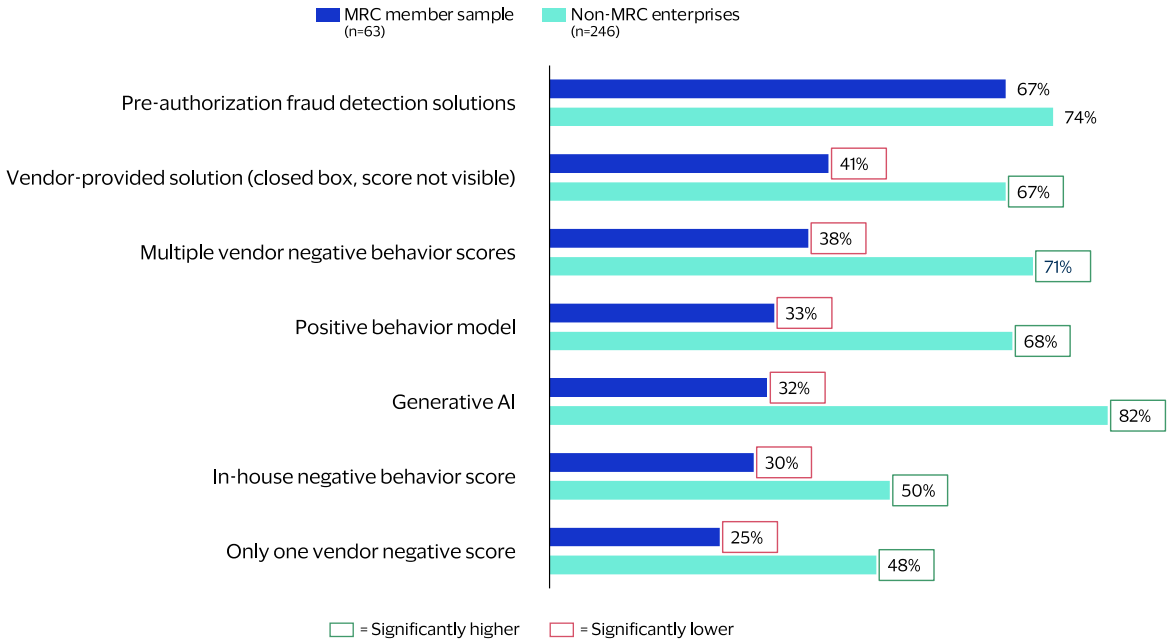
But despite these declines, these types of advanced fraud management tools are still used by sizable shares of merchants, globally with reported usage rates ranging between 26% (for single-vendor negative behavior scores) and 53% (for generative AI). And usage is likely to continue ticking upward over time, despite any short-term pullbacks, given that between 20% and 30% of those not using each tool say they are likely to add it in the next 12 months (see Figure 32).

MRC members differ significantly in their application of AI/ML tools for fraud management compared with non-MRC enterprises. In general, MRC members are far less likely to report current or planned use of nearly every one of the seven tools tested in the survey (see Figure 33). For instance, only 32% report usage of generative AI for these purposes, in contrast with 82% of non-member enterprises. The only exception to this pattern appears to be pre-authorization fraud detection solutions, which are currently used or likely to be added by 67% of MRC members and 74% of non-MRC enterprises.

© Visa 2026. All rights reserved.

Section 4: Fraud management metrics and tactics

Figure 33: Current and planned use of AI/ML fraud management tools, by MRC membership (2026, fraud professionals



Overall, the data and trends examined in this section suggest merchants are experiencing lower rates of fraud than in previous years while also pulling back on their collective use of various tools and tactics for preventing and managing fraud. It is difficult to confirm the exact relationship between these trends, i.e., whether lower fraud rates have led merchants to decrease their use of tactics and tools or whether decreases in the use of tactics and tools has led merchants to let more fraud attempts "fly under the radar," so to speak, in terms of their ability to detect and combat them.

It is also possible that both trends are taking place somewhat independently and not having much impact on each other at all. Regardless of the relationship between those trends, it seems clear that decreases in the incidence rates of fraud have not yet translated into significant improvements in most fraud-related metrics; in fact, a few indicators, including fraud rate by order and average rate of false positives, seem to be trending in the wrong direction. Merchants must remain vigilant in their approaches to screening for fraud and applying advanced tools and tactics to effectively counter this ongoing and constantly evolving threat.

© Visa 2026. All rights reserved.

Section 5:

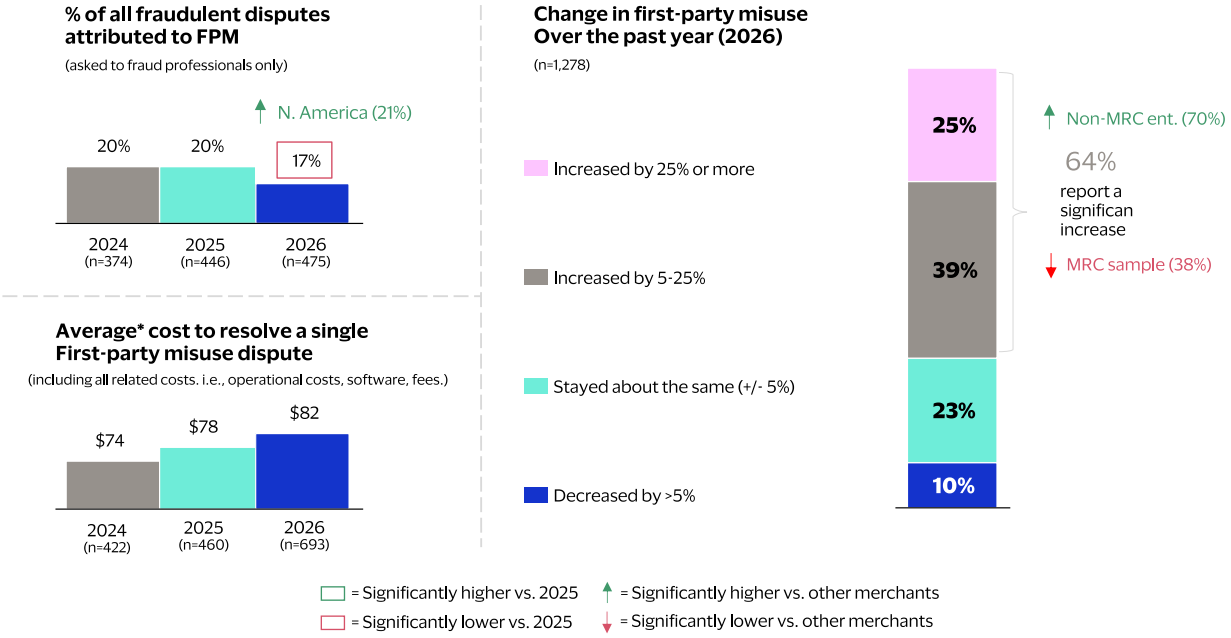
Post-purchase fraud and abuse

In this section, the focus is on two specific types of post-purchase fraud: (1) first-party misuse, which we define as fraudulent or abusive behavior committed by a customer after they receive a purchased product or service, and (2) refund/policy abuse, which we define as instances when a customer makes a transaction with a debit, credit, or prepaid card and uses cardholder dispute protections to receive an illegitimate refund. Both types of fraud have ranked among the five most widespread, in terms of the shares of merchants experiencing them in recent years of our survey, and their continued prevalence, along with the significant costs and harms they incur, merit focused attention and investment from merchants.

Most merchants report a rise in first-party misuse and the costs required to manage it

When we ask all survey respondents (both fraud and payment professionals) about the trend in first-party misuse (FPM) over the past year, most (64%) report a meaningful increase, as evidenced by the graph on the right in Figure 34. MRC members, however, are significantly less likely to report a rise in FPM, with only 38% citing any increase, in contrast to 70% of non-MRC enterprises.

Figure 34: FPM-related metrics (2024–2026, fraud and payment professionals)



Also shown in Figure 34 are two additional bar charts: The first shows the share of fraudulent disputes that merchants attribute to FPM. Overall, this figure fell significantly from 20% to 17% in this year's survey, although merchants in North America continue to report a higher level of FPM (21%), more on par with prior-year estimates.

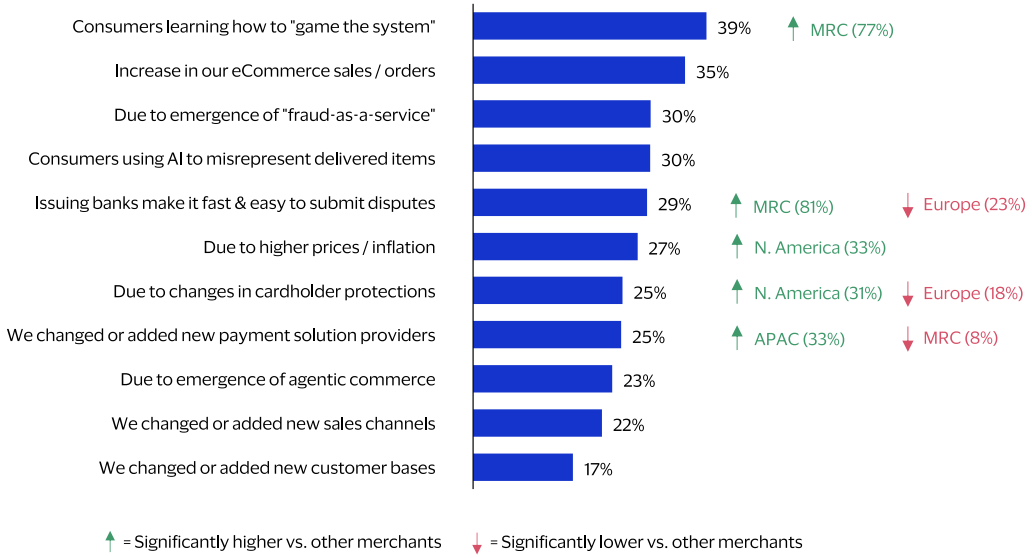
The other chart depicts merchant estimates of the average cost to resolve each FPM dispute, which has risen steadily for two years now. It currently sits at $82, exceeding the $80 mark for the first time ever in our research.

© Visa 2026. All rights reserved.

Section 5: Post-purchase fraud and abuse

Those claiming an increase in FPM this year continue to point the finger primarily at consumers learning how to "game the system." Approximately four in ten (39%) cite this as a primary reason overall, but this figure rises to nearly eight in ten (77%) among MRC merchants (see Figure 35). Increasing eCommerce sales/orders is also a common reason, with 35% citing this as a driving factor in rising FPM rates this year. A sizable share (30%) of merchants also blame newer, more advanced fraud tools and tactics for rising FPM, as well, including the emergence of "fraud-as-a-service" and consumers using AI to misrepresent delivered items.

Figure 35: Reasons why FPM is increasing (2024–2025, fraud & payment professionals)



But consumers and fraudsters aren't the only ones responsible for rising FPM, according to merchant fraud and payment professionals: nearly three in ten (29%) also point to issuing banks making it fast and easy to submit disputes as a key factor. MRC members are significantly more likely to cite this factor, with 81% saying it is driving the FPM increase. Conversely, merchants in Europe are significantly less likely to cite it.

MRC members are significantly more likely to cite this factor, with 81% saying it is driving the FPM increase.

Other drivers of increasing FPM include higher prices/inflation and changes in cardholder protection, both of which are significantly more salient for merchants in North America versus those in Europe and elsewhere. And merchants themselves take some of the blame as well, with 25% claiming that adding and changing payment partners has elevated their FPM rates. This plays a significantly greater role (33%) for merchants in APAC and a significantly smaller one (8%) for MRC members.

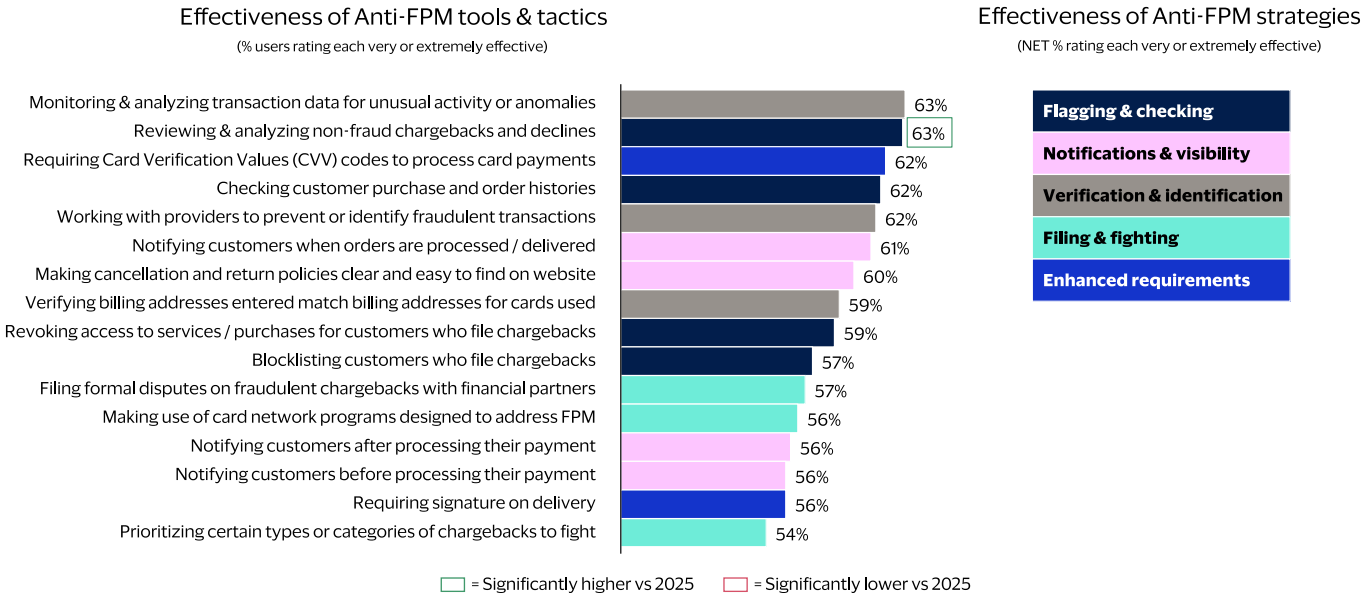
© Visa 2026. All rights reserved.

Section 5: Post-purchase fraud and abuse

Given the reported increase in FPM and the many factors merchants say are contributing to this pervasive form of fraud, what methods are they using to combat it? The data in Figure 36 sheds light on the wide range of tools, tactics, and strategies merchants currently use to combat FPM as well as their relative effectiveness.

Overall, these data indicate merchants are pulling all the levers they can to counter this type of fraud, and most are finding these tools and tactics quite effective in achieving that goal. The five most effective methods this year are monitoring and analyzing transaction data, analyzing non-fraud chargebacks and declines, requiring CVV codes for card payments, checking customer order histories, and working with providers to prevent and identify fraudulent transactions. All of these methods are rated very or extremely effective by more than 60% of merchants using them. Also, basic tactics like notifying customers when orders are processed and delivered and making merchant cancellation and return policies clear and easy to find for consumers are considered quite useful in this regard as well.

Figure 36: Effectiveness of strategies and tactics to combat first-party misuse



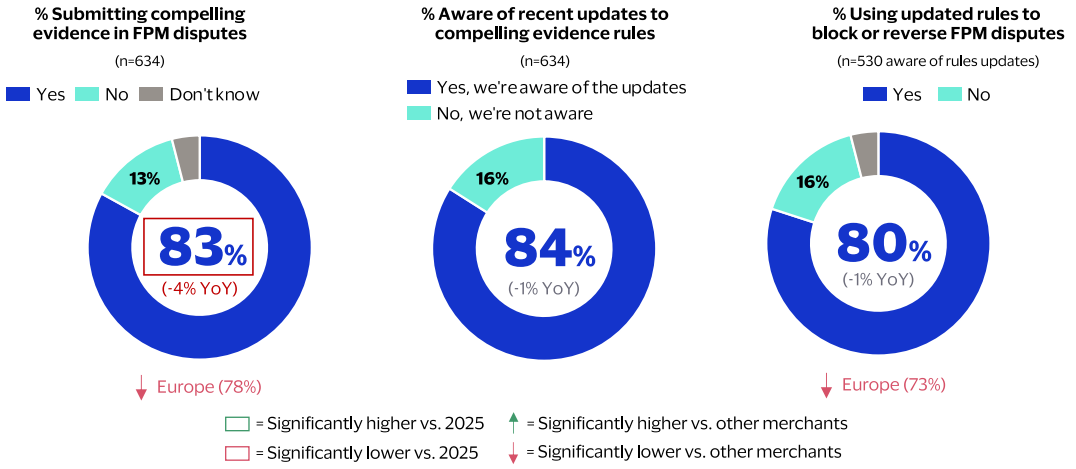
The effectiveness of all anti-FPM methods has generally stayed consistent with prior years. The sole exception is reviewing and analyzing non-fraud chargebacks and declines, which significantly more merchants rate as highly effective this year compared with last. At a high level, merchants' "all of the above" strategy for combating FPM seems to be working well, with the vast majority (76% to 88%) that use each different type of tool and tactic shown in the table in Figure 36 rating that approach as highly effective.

© Visa 2026. All rights reserved.

Section 5: Post-purchase fraud and abuse

To aid merchants in combating FPM, card brands have implemented and regularly updated their rules for submitting compelling evidence, which can help merchants tip fraudulent FPM disputes in their favor. Last year, our survey showed an uptick in the use of compelling evidence, with 87% of merchants saying they leveraged this method in FPM disputes. This year, that number ticked back downward, putting usage rates back on par with where they were in 2024, at 83% globally (see Figure 37).

Figure 37: Use of compelling evidence to fight first-party misuse (2025–2026, fraud professionals)



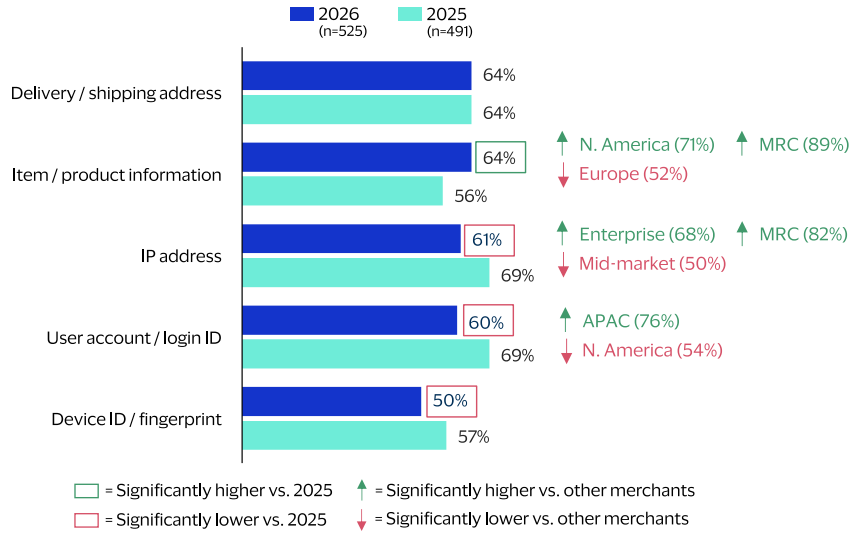
There is one major caveat here, which is that the decline in use of compelling evidence is likely driven by our shift in this year's sample distribution to include more merchants in Europe.

Our data consistently show merchants in this region are less likely to make use of compelling evidence, including use of the updated rules instituted by card brands, so including more European merchants in this year's survey certainly contributed to decrease shown in this year's results at the global level.

In any case, while the decline from 87% to 83% of merchants using compelling evidence is statistically significant, it is not really meaningful from a big-picture perspective, as more than eight in ten are still using this method to counter this particularly widespread and challenging form of fraud.

The final question fraud professionals are asked on this topic is what types of eCommerce transaction and customer data they currently collect and use as compelling evidence in FPM disputes. There are several notable shifts and skews in this year's data when it comes to this question. Compared with last year, fewer merchants cited IP addresses, user account/login IDs, and device IDs as data points they use for compelling evidence (see Figure 38). In contrast, significantly more are using item and product information as compelling evidence, as the data show nearly a 10 percentage-point increase (from 56% to 64%) year-on-year.

Figure 38: Data points used as compelling evidence (2025–2026, fraud professionals)



© Visa 2026. All rights reserved.

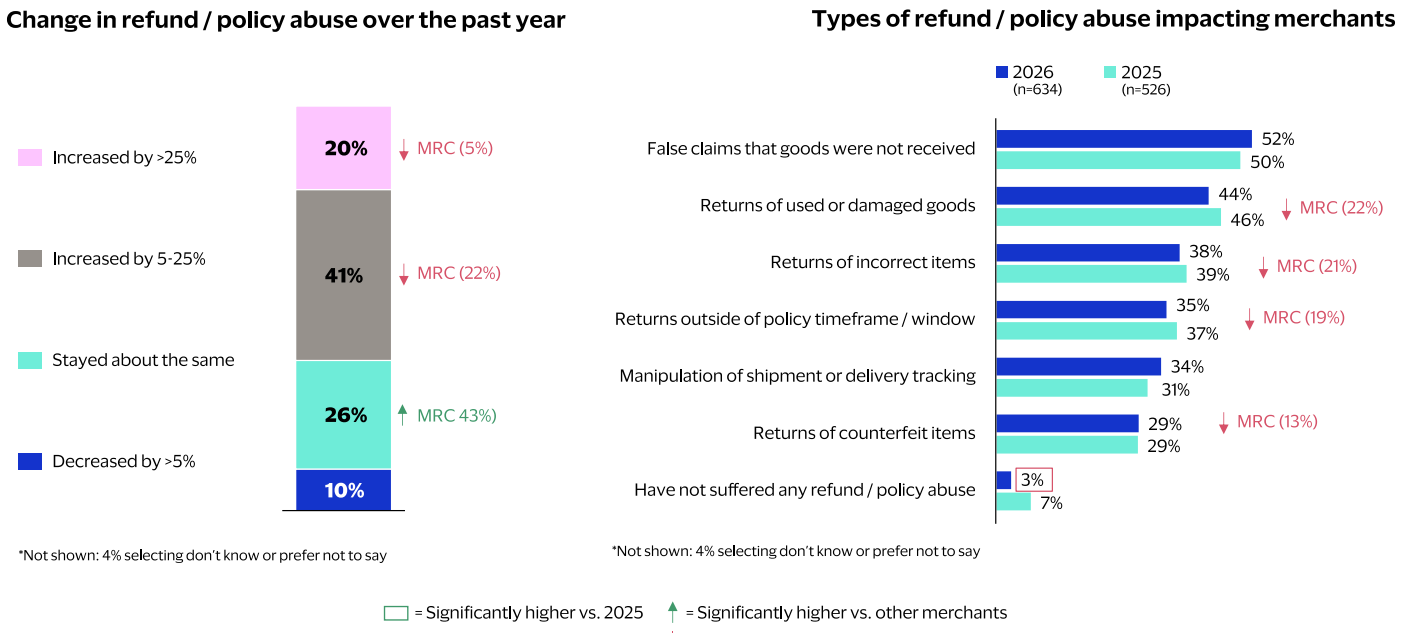
Section 5: Post-purchase fraud and abuse

The significant skews on this question among merchants in different regions and size tiers indicate that merchants are deploying a variety of different approaches to collecting and using compelling evidence data. For instance, North American merchants are more likely than others to use item and product information, while those in Europe are less likely. On the other hand, North American merchants under-index on the use of user account or login ID information, while those in APAC are significantly more likely to collect and submit this as compelling evidence.

In terms of merchant sizes, enterprises are more likely to use IP addresses while mid-market merchants are significantly less likely. And as with many other topics in this report, MRC merchants show a couple of major differences of their own in this area, as they over-index significantly on the use of item/product information and IP addresses. While the data is a bit "noisier" than usual on this subject due to the shift in sample distribution across regions, it generally indicates that compelling evidence continues to be a major tool in merchants' anti-FPM arsenals, and one that merchants in different segments and regions seem to be employing in a variety of different ways.

The final set of fraud-related insights in this report zooms in on the specific type of fraud that has the highest overall incidence, claimed by 41% of merchants this year: refund/policy abuse (see Figure 24). More than six in ten (61%) of merchants cite an increase in refund/policy abuse over the past year, with 20% citing spikes of 25% or more (see Figure 39). In contrast, only 10% cite a decrease and 26% say the rate of this type of fraud has remained fairly consistent year to year.

Figure 39: Trends in refund/policy abuse (2025-2026, fraud professionals)



When asked what kinds of refund/policy abuse they are experiencing, most (52%) call out false claims that goods were not received. More than one-third also cite returns of used, damaged, or incorrect items, late returns outside of the policy timeframe, and manipulation of shipping/delivery tracking information (see Figure 39).

Notably, MRC merchants seem to be struggling far less with refund/policy abuse. They are less likely to report any increase in this type of fraud (only 28% say this) and more likely to say they their rates of refund/policy abuse are staying flat. Also, MRC merchants are less likely to report experiencing this kind of fraud via illegitimate returns, i.e., returns of used, damaged, incorrect, or counterfeit items and late returns. These data points indicate MRC merchants may be better able to counter refund/policy abuse, at least when it comes to return-based attempts at this kind of fraud.

© Visa 2026. All rights reserved.

Conclusion

Overall, this year's survey of payment and fraud professionals offers a wealth of fresh data, insights, and findings that collectively convey how complex and challenging it is for merchants to effectively manage these aspects of the eCommerce business in the current global marketplace.

Payment acceptance offerings continue to gradually evolve as merchants increasingly offer customers new, convenient options like real-time payments, and soon, agentic AI payments. Merchants continue to track a broad range of key payment metrics and utilize a wide array of tools, techniques, and tactics to optimize payment efficiency, security, and experiences for customers. These include encouraging customers to pay with preferred methods, employing various tools and techniques to increase authorization rates, and leveraging tokenization to protect and delight customers.

As merchants work to optimize payment acceptance, they must also remain tireless and vigilant in their efforts combat fraud. While this year's survey again shows encouraging signs that payment fraud may be on the decline, merchants are also facing new challenges, including growing financial pressures, complicated data and technology difficulties, and increasingly strained internal resources. Gaining cost and time efficiencies,

As merchants work to optimize payment acceptance, they must also remain tireless and vigilant in their efforts combat fraud.

working out kinks in the fraud management tech stack, orchestrating and optimizing fraud platforms and solutions, and generally staying alert and up to date on the fast-evolving matrix of fraud threats are all major imperatives for merchant fraud professionals moving forward.

© Visa 2026. All rights reserved.

About the authors

Visa Acceptance Solutions, a Visa solution, is for businesses looking to build the payments experiences of the future. We leverage the power of Cybersource, Visa security, and innovation to provide end-to-end payment, authentication, fraud, risk, and dispute solutions, create seamless customer experiences, and power global growth. With 60+ years of payments expertise, Visa Acceptance Solutions' leading-edge technologies, flexible infrastructure, and data-driven approach can help businesses thrive.

Verifi, a Visa solution, is a leading provider of next generation post-purchase solutions, that streamline the dispute process and improve the customer experience. Available for all major card brands, Verifi solutions help merchants globally to prevent and resolve disputes by sharing compelling evidence, data transparency and merchant-initiated or rules-based refunding. Verifi equips merchants, issuers and acquirers to reduce financial loss, create operational efficiencies, and remove unnecessary fraud and first-party misuse disputes from the payment ecosystem.

For more information, please visit: visaacceptance.com or verifi.com.

The Merchant Risk Council (MRC) is a non-profit global membership organization dedicated to connecting eCommerce fraud prevention and payments professionals. It offers a range of resources, including educational programs, online community groups, conferences, and networking events. With over 750 member companies, including more than 500 merchants, the MRC delivers valuable insights on fraud prevention, payments optimization, and risk management. Founded in 2000, the MRC remains a leading force in the industry, driving the evolution of eCommerce by promoting payments optimization and reducing fraud through collaboration, education, networking, and advocacy.

For more information, please visit: merchantriskcouncil.org.

B2B International is a global, full-service market research firm, specializing in researching B2B markets. We help our clients achieve their business goals by making smarter decisions, driven by insights.

B2B International is part of Merkle B2B. At Merkle B2B, we partner with some of the world's biggest brands to power world-class business experiences that inspire people, grow businesses, and deliver transformative outcomes.

For more information, please visit: b2binternational.com.

© Visa 2026. All rights reserved.

Appendix 1:

Payment method conversion and acceptance rates

To aid merchants and payment partners with useful quantitative benchmarks on specific payment methods, two tables are shown below that show average conversion and acceptance rates by method (estimated by payment professionals in this year's survey):

Figure 40: Average payment method conversion rates, by region, size and MRC membership (2026, payment professionals)

Average conversion rate* by payment method (mean** / median)	Overall		Region								Size						Membership			
			North America		Europe		Asia Pacific		Latin America		SMB		Mid-Market		Enterprise		MRC Sample		Non-MRC Enterprises	
Cards	40%	38%	41%	40%	46%	40%	34%	24%	36%	32%	38%	35%	43%	40%	39%	30%	79%	80%	36%	25%
Digital wallets / eWallets	36%	25%	36%	25%	39%	30%	34%	25%	30%	20%	29%	20%	38%	25%	37%	30%	75%	80%	35%	25%
Bank transfers / direct debit	33%	25%	33%	22%	38%	30%	28%	20%	33%	30%	33%	29%	36%	25%	32%	20%	72%	70%	30%	20%
mCommerce Mobile Payments	32%	20%	37%	25%	32%	25%	28%	20%	30%	20%	32%	25%	29%	20%	33%	20%	58%	70%	32%	20%
Real-Time Payments	31%	20%	34%	20%	34%	20%	25%	17%	34%	20%	34%	25%	33%	20%	29%	20%	88%	88%	28%	20%
Cash	31%	20%	31%	20%	38%	25%	27%	18%	25%	18%	31%	20%	31%	20%	30%	20%	75%	78%	29%	20%
Buy Now Pay Later	28%	20%	32%	20%	28%	20%	24%	13%	22%	15%	37%	32%	28%	15%	25%	20%	77%	83%	22%	16%
Gift cards / vouchers	27%	15%	30%	20%	21%	15%	29%	15%	23%	15%	24%	15%	25%	15%	30%	20%	96%	95%	25%	15%
Other local payment methods (Boleto, Neosurf, Pix, POLi, etc.)	26%	20%	49%	55%	23%	15%	15%	5%	27%	25%	27%	28%	27%	25%	27%	14%	64%	90%	21%	10%
Cash on Delivery	23%	20%	25%	15%	29%	20%	22%	19%	14%	10%	27%	20%	22%	15%	23%	20%	--	--	23%	20%
Cryptocurrency / Stablecoins	20%	15%	20%	15%	23%	16%	17%	10%	19%	16%	20%	10%	27%	20%	17%	11%	2%	2%	17%	11%

*Conversion rate defined as "percentage of visits from the checkout page that result in a completed checkout."
**Trimmed averages shown for means.

= Significantly higher vs. other segments = Significantly lower vs. other segments

Figure 41: Average payment method acceptance rates, by region, size and MRC membership (2026, payment professionals)

Average conversion rate* By payment method (mean** / median)	Overall		Region								Size						Membership			
			North America		Europe		Asia Pacific		Latin America		SMB		Mid Market		Enterprise		MRC Sample		Non-MRC Enterprises	
Cards	57%	60%	63%	75%	60%	60%	47%	30%	56%	50%	56%	60%	60%	60%	57%	53%	90%	90%	53%	46%
Bank Transfers / Direct Debit	54%	50%	62%	80%	55%	50%	43%	25%	56%	53%	57%	50%	55%	50%	52%	40%	94%	98%	49%	35%
Digital Wallets / eWallets	53%	48%	59%	75%	57%	63%	42%	25%	52%	45%	55%	55%	55%	50%	52%	40%	93%	95%	49%	30%
Cash	51%	30%	58%	55%	52%	35%	37%	20%	58%	55%	59%	70%	54%	40%	45%	24%	78%	100%	45%	23%
Real-Time Payments	50%	35%	60%	80%	48%	40%	37%	20%	57%	80%	55%	50%	52%	38%	47%	30%	93%	94%	45%	25%
mCommerce Mobile Payments	49%	35%	58%	65%	49%	40%	35%	20%	55%	63%	52%	42%	50%	40%	47%	30%	93%	95%	45%	30%
Gift Cards / Vouchers	49%	32%	56%	68%	41%	25%	45%	21%	51%	65%	43%	25%	50%	55%	51%	34%	93%	95%	46%	25%
Buy Now Pay Later	46%	30%	52%	48%	45%	34%	37%	19%	55%	55%	46%	44%	50%	40%	44%	25%	90%	90%	40%	20%
Cash on Delivery	40%	20%	55%	50%	42%	30%	33%	15%	34%	20%	52%	55%	40%	20%	36%	20%	--	--	--	--
Cryptocurrency / Stablecoins	35%	20%	39%	25%	35%	25%	24%	10%	41%	20%	39%	15%	42%	30%	30%	20%	--	--	--	--
Other local payment methods (Boleto, Neosurf, Pix, POLi, etc.)	43%	30%	81%	87%	30%	15%	12%	6%	52%	50%	42%	33%	45%	30%	44%	20%	94%	96%	35%	13%

*Acceptance rate defined as "percentage of initiated payments accepted by the payment provider."
**Trimmed averages shown for means

= Significantly Higher vs. Other Segments = Significantly Lower vs. Other Segments

© Visa 2026. All rights reserved.

Appendix 2:

Survey questions used in report figures

This section shows all survey questions asked to merchants in order to gather the data shown in each numbered figure throughout this report.

Figure 1
In which country are you located?

Figure 2
Please estimate your organization's annual eCommerce revenue.

Figure 3
Which ONE of the following describes your organization's primary source of eCommerce revenue?

Figure 4
Which of the following types of payment methods does your organization currently accept?

And which of these payment methods, if any, did your organization add over the past 12 months?

Figure 5
And which of these payment methods, if any, did your organization add over the past 12 months?

For which reasons did your organization add new types of payment methods over the past 12 months?

Figure 6
Which of the following types of payment methods does your organization currently accept?

Figure 7
Which of the following types of payment methods does your organization currently accept?

Figure 8
Does your organization have one or more payment methods that you prefer or encourage your customers to use?

Figure 9
In what ways does your organization encourage or guide customers to use your preferred types of payment methods?

What is the ONE most important reason why you encourage customers to use your preferred payment method(s)?

Figure 10
Please indicate how much you disagree or agree with each statement about the usage of real-time payments among your organization's eCommerce customers.

Figure 11
How likely is your organization to add real-time payments as an acceptance method in the next 12 months?

Figure 12
Which third-party marketplaces does your organization currently use to sell to customers?

Why does your organization utilize third-party marketplaces?

Figure 13
Which third-party marketplaces does your organization currently use to sell to customers?

Figure 14
How many payment gateway or processor connections does your organization currently support?

How many merchant acquiring banks does your organization currently use?

For what reasons does your organization have multiple acquiring relationships?

Figure 15
How important are each of the following payments management key performance indicators (KPIs) to your organization?

Figure 16
Which of the following payments management key

© Visa 2026. All rights reserved.

Appendix 2: Survey questions used in report figures

performance indicators (KPIs) are extremely important to your organization?

Figure 17
Which types of payment tokenization, if any, does your organization currently use?

Note: By payment tokenization, we mean replacing sensitive customer information with a unique identifier, using gateway tokens sponsored by payment gateways, acquirers, etc. or network tokens sponsored by major card networks.

Figure 18
For which of the following reasons does your organization use payment tokenization?

Figure 19
For which of the following reasons does your organization use payment tokenization?

Figure 20
Which of the following authorization-related approaches and techniques does your organization currently use?

Does your organization use any third-party data in association with any of these?

Figure 21
Which of the following types of fraud has your organization experienced in the past 12 months?

Figure 22
Which of the following types of fraud has your organization experienced in the past 12 months?

Figure 23
Which of the following types of fraud has your organization experienced in the past 12 months?

Figure 24
Please indicate the percentage of your annual eCommerce revenue lost due to payment fraud globally - i.e., fraud rate by revenue.

Please estimate the global percentage of accepted eCommerce orders that turned out to be fraudulent (i.e., fraud rate by order), over the past 12 months.

Please estimate the share of your organization's total eCommerce transactions ultimately rejected due to suspicion of fraud over the past 12 months.

Please estimate the share of fraud-coded chargebacks and disputes your organization wins.

Note: A chargeback is defined as a transaction reversal made by an issuer when a cardholder claims fraudulent activity.

Figure 25
Please estimate your rate of false positives (also called 'customer insults') on eCommerce orders.

Figure 26
Over the past 12 months, has your organization experienced an increase in first-party misuse?

For what reasons do you believe your organization has seen an increase in first-party misuse disputes over the past year?

Figure 27
Over the past 12 months, has your organization experienced an increase in first-party misuse?

Figure 28
Over the past 12 months, has your organization experienced an increase in first-party misuse?

For what reasons do you believe your organization has seen an increase in first-party misuse disputes over the past year?

Figure 29
On average, how much does it cost your organization to resolve a (single) first-party misuse dispute?

Which of the following reasons do you believe causes first-party misuse to occur in your organization's eCommerce business?

What percentage of all fraudulent disputes do you believe are first-party misuse?

Figure 30
When thinking about methods of combating first-party misuse, how effective are each of the following methods?

Figure 31
When thinking about methods of combating first-party misuse, how effective are each of the following methods?

© Visa 2026. All rights reserved.

Appendix 2: Survey questions used in report figures

Figure 32
Do you submit compelling evidence to respond to first-party misuse disputes?

Have you heard of major card brands' 2023 updates to compelling evidence rules related to first-party misuse disputes?

Which of the following data points do you currently collect and use for compelling evidence related to first-party misuse disputes?

Has your organization used card brands' updated compelling evidence rules to block or reverse first-party misuse disputes?

Figure 33
Over the past 12 months, has your organization experienced an increase in refund / policy abuse?

Over the past 12 months, what types of refund / policy abuse have impacted your organization?

Figure 34
Over the past 12 months, has your organization experienced an increase in refund / policy abuse?

Figure 35
How important are each of the following priorities in guiding your organization's approach to fraud management?

Figure 36
How do you expect your organization's spending to change over the next two years, when it comes to each of the following areas of investment?

Figure 37
Over the past 12 months, which of these challenges has negatively impacted your organization's ability to manage fraud?

Figure 38
Thinking ahead to the next 12 months, which of the following are areas of improvement for your organization, when it comes to fraud management?

Figure 39
Approximately what percentage of your organization's total eCommerce orders do you screen for fraud.

And out of all the eCommerce orders your organization screens manually, what percentage are subsequently declined?

Figure 40
At which of the following stages in the eCommerce customer journey does your organization use a tool or signal to identify potential fraud?

Figure 41
At which of the following stages in the eCommerce customer journey does your organization use a tool or signal to identify potential fraud?

Figure 42
Which of the following types of AI/machine-learning tools and techniques does your organization currently use in its fraud strategy?

Figure 43
Which of the following types of AI/machine-learning tools and techniques does your organization currently use in its fraud strategy?

© Visa 2026. All rights reserved.