2025 Global eCommerce

Payments & Fraud Report

See survey results on:

- Payment acceptance
- Payment metrics and tactics
- Fraud attacks and metrics
- Post-purchase fraud and abuse
- Fraud management

VISA Acceptance Solutions

cybersource A Visa Solution

VERIFI A Visa Solution

MRC

Contents

Overview

In partnership with the Merchant Risk Council [MRC], the Visa Acceptance Solutions and Verifi teams are proud to present the results of the 2025 Global eCommerce Payments & Fraud survey. The purpose of this report is to convey transparent, unbiased research on merchants' views regarding current trends and challenges in the realm of eCommerce payments and fraud.

This year's report is based on our annual global survey of over 1,000 total eCommerce merchants. The survey sample includes a diverse mix of small-business [SMB], mid-market, and enterprise merchants representing organizations based in over 35 countries throughout North America and Europe, as well as the Asia-Pacific [APAC] and Latin America [LATAM] regions. In addition to this year's survey, we also leverage trended survey data from previous years to understand not just where merchants stand on various issues today but also how their views have been changing over time and how they may further evolve in the near future. The next section of the report provides further details on the research methodology and survey sample.

Leveraging our robust survey dataset, this report delves into the eCommerce payments landscape to shed light on the payment acceptance and payment management practices that merchants are deploying, as well as the key challenges and improvement areas that merchants will be focused on throughout 2025. In addition, the report offers the MRC merchant community the latest industry fraud data and fraud management methods used by their peers, along with a robust set of performance benchmarks that members can use to help optimize their fraud management and prevention practices.

Survey methodology and sample

The survey for this year's report was fielded in October to November of 2024. In total, 1,082 merchant professionals involved in eCommerce payment and fraud management (including 70 MRC members) completed the survey. The respondent sample includes fraud and payment professionals based in 38 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.

Among the 70 MRC members participating in this year's survey sample, around six in 10 (57%) are based in North America, with the remainder based primarily in Europe (24%). The vast majority (at least 74%) of MRC respondents are fraud and payments professionals at large enterprise merchants – i.e., those generating over $50 million in annual eCommerce revenue.

Figure 1

Share of sample by geographic region

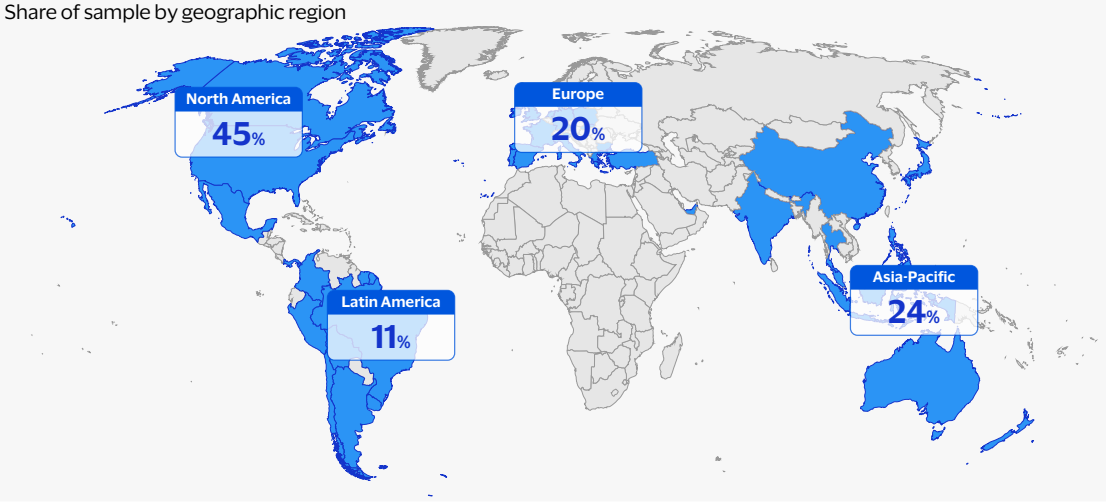
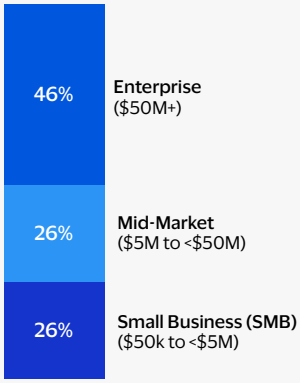


Figure 2

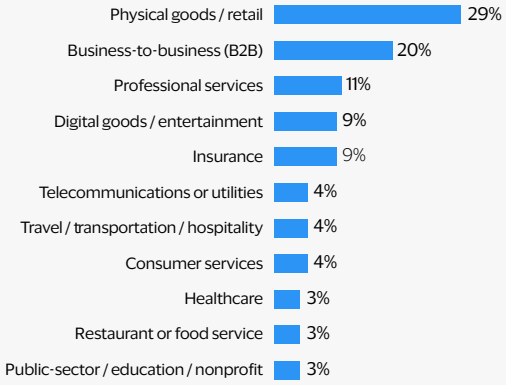
Share of sample by merchant size (based on annual eCommerce revenue)



2%: Prefer not to say

Figure 3

Share of sample by primary eCommerce category



1%: Other goods or services not listed above

Executive summary

The key insights from the 2025 Payments & Fraud report 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.

This section summarizes the key learnings emerging from all five sections in the report, providing a high-level overview of all the major changes, trends and headlines revealed by our most recent research:

1. Payment acceptance

Merchants keep acceptance offerings consistent, while showing rapid uptake of real-time payments (RTPs)

- Merchants continue to accept a handful of different payment methods, with the majority taking cards, eWallets, and debit transfers. Over one-third also accept mCommerce, RTP, and buy-now-pay-later (BNPL) payments.
- Roughly one-quarter added no new payment methods this year, signaling increased consistency in acceptance offerings.
- Globally, 37% currently accept RTPs, and a large share (42%) of the rest are likely to implement RTP this year.
- Among merchants currently accepting RTP, ~80% saw a marked increase in the use of this method by their customers over the past year, and ~90% expect a similar uptick next year.

Card, digital wallet, and real-time payments are widely preferred and promoted

- 90% of merchants have preferred payment methods they encourage eCommerce customers to use, typically through promotions and incentives at checkout.
- Minimizing fraud risks and processing costs are the two main reasons merchants prefer the methods above.
- MRC members are less likely to have preferred methods, but those that do often cite increased conversion as the rationale.

Marketplaces, gateways, acquirers remain key partners for supporting acceptance and maximizing sales

- Third-party marketplaces remain key sales and acceptance partners, especially for midsize merchants.
- While Amazon is used widely in all regions, use of other marketplaces varies dramatically by geography.
- Merchants also use multiple (usually 3 to 4) payment gateways and acquiring banks, both for overall flexibility and to maximize authorizations.

2. Payment metrics and tactics

Key payment indicators abound, but seven stand out as most critical for merchants

- Out of 14 payment metrics tested in this year's survey, over 50% of merchants rate every metric "very or extremely important" to their organization.
- But six metrics stand out as "extremely important" to over 4 in 10, globally: revenue, success rate, loss rates, authentication rate, authorization rate, and cost of payments. Loss rate, in particular, has grown significantly in importance, over the past year. And there is a seventh metric — cost of service / cost per customer – that stands on the cusp of joining this set of "core payment indicators," as well (sitting just below the threshold, with 39% of merchants rating it extremely important).
- SMBs and MRC members focus mainly on the most critical metrics, while larger merchants and non-MRC enterprises consider a wider range of KPIs to be highly important to their business.

Authorization and tokenization tactics persist, especially among large merchants

- Over 90% use various approaches to boost authorization rates, with Strong Customer Authentication (SCA) one of the most popular (used by 40%).
- 6 in 10 merchants use tokenization in payments to reinforce payment security, boost authorization rates, and enable convenient payment experiences.
- Network tokens are becoming a more popular form of tokenization as gateway tokens decline in usage.
- Merchants employ tokens mainly to reinforce payment security, boost authorization rates, and enable innovative, convenient payment experiences for customers online.
- Use of these tactics varies drastically by merchant size (enterprises lead the way).

See how Token Management Service can help you reinforce security, enable network tokens to boost authorization rates, and power innovative shopping experiences. Learn more here.

3. Fraud attacks and metrics

Fraud rates are down, with significant declines in first-party misuse, card testing & triangulation schemes

- Fraud rates are down across the board, reversing a multi-year trend of increasing incidence.
- Significant declines reported in incidence of first-party misuse, card testing, and triangulation schemes.
- The dip in first-party misuse is notable, as this form of fraud has risen rapidly over the past two years.
- Real-time payment fraud, refund/policy abuse, phishing attacks, first-party misuse and card testing are the top five threats. These attacks each impact between one-third and half of all merchants globally.
- 98% of merchants report experiencing one or more types of fraud in the past 12 months.
- MRC members over-index significantly on experiencing these types of fraud, while non-MRC members over-index only when it comes to identity theft.

Other fraud-related metrics also show improvement

- Additional fraud metrics show marginal year-over-year improvements.
- Order rejection rates declined significantly over the past year.
- Merchants also made progress cutting down on false positive (or "customer insult") rates, with a significant decline in the share reporting rates above 10%.

MRC members lead the way in fraud prevention, reporting better metrics despite registering more attacks

- Despite experiencing more attacks each year, MRC members report significantly better fraud metrics than non-MRC enterprises, including:
  - Lower fraud rates by order and by revenue
  - Lower rejection rates
  - Higher dispute win rates
  - Lower false positive rates

4. Post-purchase fraud and abuse

First-party misuse slows and evolves, with merchants shifting more blame to customers and issuers

- 6 in 10 report increasing rates of first-party misuse (FPM), but significantly fewer saw a major spike this year.
- Merchants cite a few new drivers of rising first-party misuse this year, attributing it mainly to consumers learning how to "game the system" and to issuing banks making it too easy to submit and win disputes (versus last year's top reasons of general inflation, changes in cardholder protections, and changes in customer/payment partners).

Uptake of anti-FPM tools and tactics continues, with nearly 90% making use of compelling evidence

- The slowdown in FPM may be driven partly by the steady uptick in the shares of merchants using compelling evidence to block and reverse fraudulent disputes.
- Nearly 90% of merchants now use compelling evidence (up from 83% last year), and more merchants are current on the latest rules and using the full array of relevant data points to combat these disputes.
- Use of many anti-FPM tools and tactics is also increasing, slowly but steadily.
- Notably, MRC members see the issue of FPM somewhat differently than non-member enterprises, reporting a significantly higher share of fraudulent disputes as FPM but also paying significantly less to resolve them. Members are much more pessimistic about the effectiveness of various anti-FPM tools and tactics, and they are also more likely to make the most use of compelling evidence by submitting additional relevant data points when disputing suspicious transactions.

See how Verifi can help identify and block confirmed first-party misuse with data transparency and enhanced merchant and transaction detail. Learn more here.

Refund/policy abuse now on the rise, adding to merchants' post-purchase problems

- Over half (57%) report increasing rates of refund/policy abuse, with over one-fifth (22%) citing increases of 50% or more over the past year.
- Merchants say this is mainly driven by false claims that goods were never received, as well as attempted returns of used, damaged, or incorrect items.
- This form of fraud is significantly more likely to affect merchants in APAC, as well as enterprise.

5. Fraud management strategies and tactics

Reducing fraud remains the primary imperative, but more are aiming to achieve cost reductions in 2025

- Reducing fraud and chargebacks remains the top strategic priority for merchant fraud professionals.
- But reducing operational costs of fraud management has grown significantly more important to some, over the past year.

Survey shows increasing reliance on data and technology to fight fraud

- Compared with last year, merchants are screening fewer orders manually and more orders digitally.
- Out of all manually screened orders, merchants end up declining roughly 20% (consistently across segments).
- Order screening rates vary significantly by region, merchant size, and MRC membership as well as eCommerce category.
- Most merchants digitally monitor for fraud at the purchase/payment stage of the customer journey and at the refund/dispute stage – in fact, the latter percentage rose significantly over the past year, from 45% to 57%.
- Yet the majority still do not monitor for fraud at other stages of the buying cycle, including at delivery/pickup.
- Merchants are quickly embracing generative AI fraud tools: over half already use them, and many more plan to start soon.
- Improving the accuracy of AI/ML fraud tools and increasing automation of fraud prevention are top improvement areas that merchants plan to focus on in 2025.

Results also indicate intensified focus on data- and technology-related challenges and improvements

- Over 80% struggle with data and tech challenges, such as effectively using data, improving accuracy of AI/ML tools, and overcoming gaps in fraud tool features/capabilities.
- Merchants also struggle to stay current on the latest threats and to constantly adapt tools and tactics.
- Looking ahead, 63% plan to ramp up spending on tools and technologies (versus half planning to spend more on staff/talent).

Learn how our risk score and AI fraud solutions recognize patterns in vast datasets to help deliver a more personalized payment experiences.

1. Payment acceptance

The first two sections of this report offer survey insights on various topics related to eCommerce payments. Specifically, these sections illuminate how merchants are being paid by customers, which payment tactics and metrics are integral to their business, and what kinds of third-party partners and enablers they rely on to support payment experiences and operations.

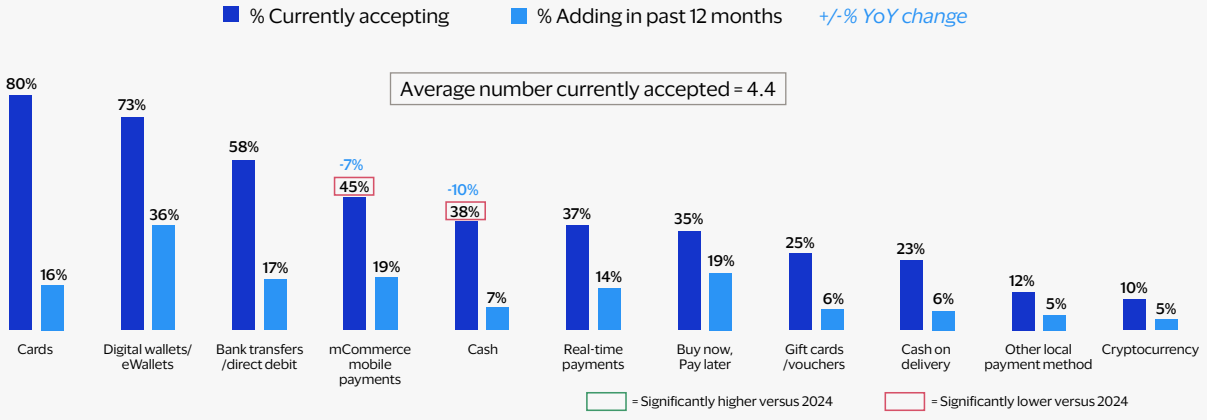
This section focuses on payment acceptance – i.e., which payment methods merchants are accepting, what their views and approaches are when it comes to adopting new payment methods, including real-time payments (RTP), and how third-party partners like online marketplaces, payment gateways/processors and acquiring banks support payment acceptance.

Acceptance offerings remain consistent, although real-time payments are poised for growth

Consistent with prior years of our study, merchants continue to accept four to five different payment methods, on average, from their eCommerce customers (see Figure 4). Card, digital wallet, and bank transfer/debit payments are the most widely accepted methods, each offered by over half of merchants worldwide. Roughly 4 in 10 merchants also accept mobile payments (45%) and cash (38%), although acceptance rates for these two methods are down significantly, versus last year.

Figure 4

Payment methods currently accepted/added in past year (2025, payment professionals)

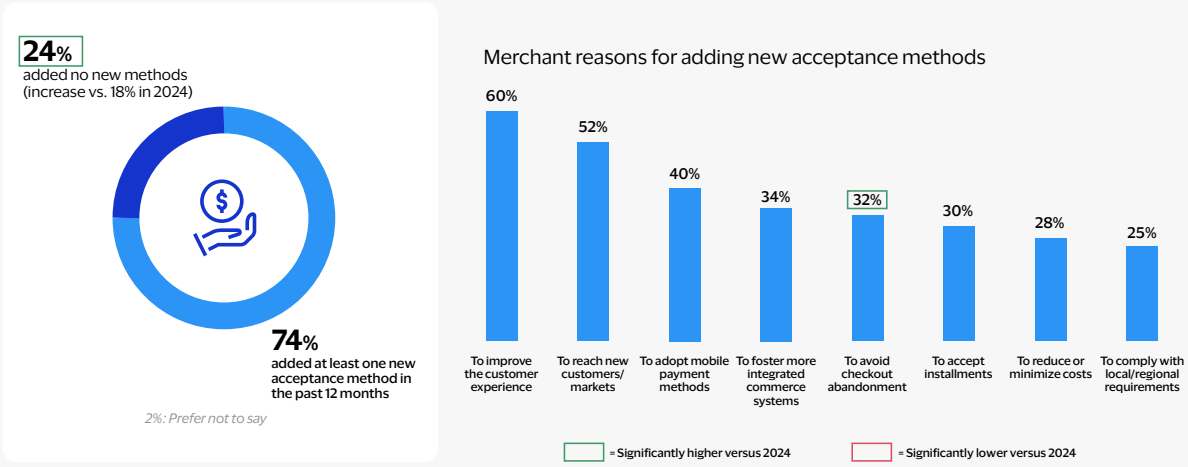


As consumer expectations and preferences regarding digital payments evolve, so too must merchant acceptance offerings. Among the fastest-growing new payment methods in 2025 are digital wallets (currently accepted by 73%), BNPL (accepted by 35%), mobile payments (accepted by 45%) and bank transfers (accepted by 58%). Among the total share of merchants that currently accept each of these methods, a sizable share (at least 17%) report adding them just in the past year (see Figure 4).

Overall, nearly three-quarters (74%) of merchants report adding at least one new payment method in the past 12 months (see Figure 5). The main reasons merchants add new payment methods are to improve the customer experience and to reach new customers or markets. Compared with last year, more merchants are also adding payment methods to avoid or reduce abandoned carts at checkout (32% cite this reason this year, versus 24% in 2024).

Figure 5

Payment methods currently accepted by MRC membership (2025, payment professionals)



While the top three most widely accepted methods are all used by the majority of merchants, worldwide, the survey data do show significant variation in acceptance offerings by region and size segment. As depicted in Figure 6, merchants in Asia are significantly less likely than those in other regions to accept card payments, but they are more likely than those elsewhere to accept cash on delivery. Merchants in Asia and Europe over-index on accepting debit transfers, compared to those in North and Latin America. And merchants in Latin America are less likely to offer buy-now-pay-later (BNPL) payments but more likely than those in all other regions to accept alternative, local payment methods, like Pix and Boleto.

Figure 6

Payment methods currently accepted by MRC membership (2025, payment professionals)

% Merchants currently accepting each method	Overall	By region				By size		
		North America	Europe	Asia-Pacific	Latin America	SMB	Mid-market	Enterprise
Base	*562*	*211*	*143*	*108*	*95*	*142*	*138*	*269*
Cards	**80%**	81%	85%	67%	85%	83%	84%	75%
Digital wallets/eWallets	**73%**	75%	77%	66%	68%	65%	68%	78%
Bank tranfers/direct debit	**58%**	50%	66%	69%	53%	53%	51%	65%
mCommerce mobile payments	**45%**	45%	45%	46%	45%	42%	48%	45%
Cash	**38%**	42%	29%	39%	39%	46%	32%	36%
Real-time payments	**37%**	37%	36%	41%	33%	37%	32%	39%
Buy now, pay later	**35%**	38%	43%	35%	17%	20%	36%	42%
Gift cards/vouchers	**25%**	27%	24%	26%	21%	14%	25%	29%
Cash on delivery	**23%**	21%	21%	33%	16%	19%	26%	23%
Other local payment methods (Boleto, Neosurf, Pix,POL, etc)	**12%**	7%	10%	6%	31%	6%	9%	16%
Cryptocurrency	**10%**	12%	6%	7%	13%	8%	8%	12%
Average number accepted	**4.3**	**4.4**	**4.4**	**4.4**	**4.2**	**3.9**	**4.2**	**4.6**

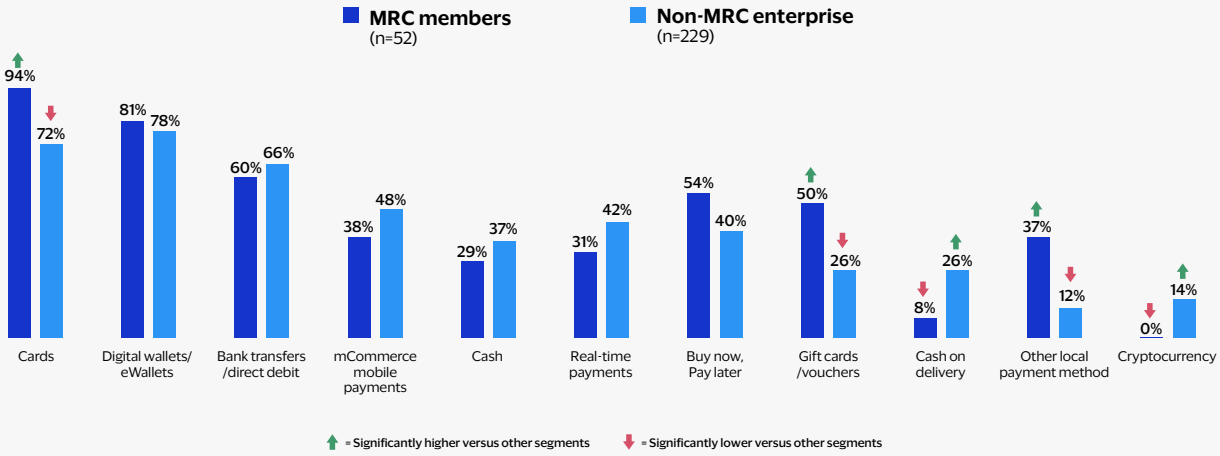
= Significantly higher versus other segments = Significantly lower versus other segments

Acceptance offerings also vary by merchant size. SMBs and mid-market merchants accept significantly fewer methods, on average, than enterprises, although SMBs do over-index relative to the larger segments on accepting payments in cash. Enterprise merchants over-index on acceptance of digital wallets, debit transfers, BNPL, gift cards, and other local methods.

There are also significant differences between MRC members and non-MRC enterprises, in terms of their payment acceptance offerings (see Figure 7). In general, MRC merchants are far more card- and wallet-focused in their acceptance offerings, while non-MRC enterprises are more likely to accept payments via newer and more "niche" methods, such as cash on delivery and cryptocurrency. MRC members also over-index on offering gift cards/ vouchers and alternative payment methods.

Figure 7

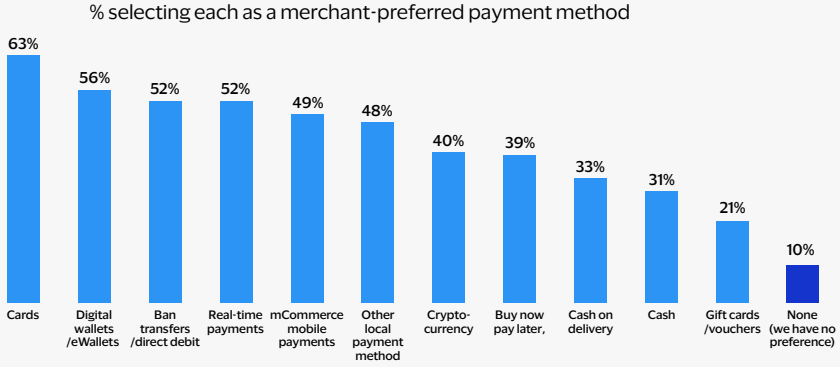
Payment methods currently accepted by MRC membership (2025, payment professionals)



When asked which payment methods they prefer to accept from eCommerce customers, the majority of merchants point to cards, digital wallets, debit transfers, and RTP, and just under half cite mCommerce mobile payments and other local payment methods (see Figure 8). Gift cards and vouchers are least preferred, followed by cash and cash on delivery. Globally, these three methods are preferred by only one-third of merchants or less.

Figure 8

Merchant-preferred payment methods (2025, payment professionals accepting each method)

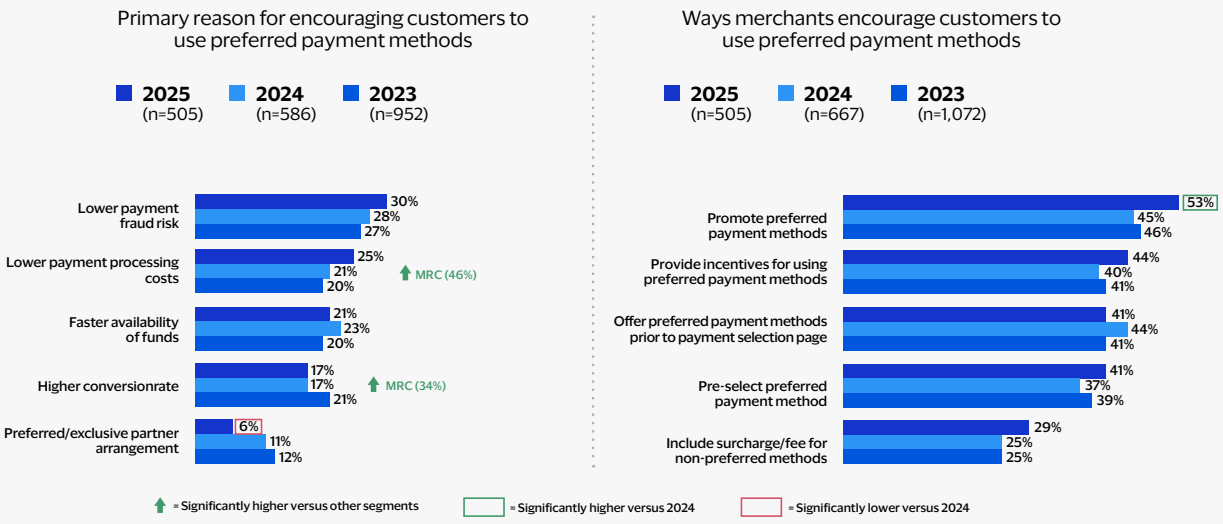


Why do merchants prefer certain payment methods? For the past three years, merchants have offered a relatively consistent set of reasons, with lower payment fraud risk and lower processing costs serving as the primary motivators for most (see Figure 9). Notably, MRC merchants are significantly more likely than other merchants to encourage customers to use certain payment methods to save on processing costs and to maximize conversion rates.

As for how they encourage customers to use their preferred methods, merchants employ several tactics. The majority (53%) promote these methods visually and/or with messaging on checkout and payment pages. Other popular tactics include providing incentives for using preferred methods (selected by 44%), offering preferred methods prior to the main checkout page (41%), and pre-selecting preferred methods by default, when customers are checking out and paying for their purchases (41%). The least popular method is applying the "stick" of an extra surcharge or fee for those paying with non-preferred methods, but even this somewhat punitive tactic is utilized by nearly three in 10 merchants (29%).

Figure 9

Encouraging customers to use preferred payment methods (2023-2025, payment professionals)



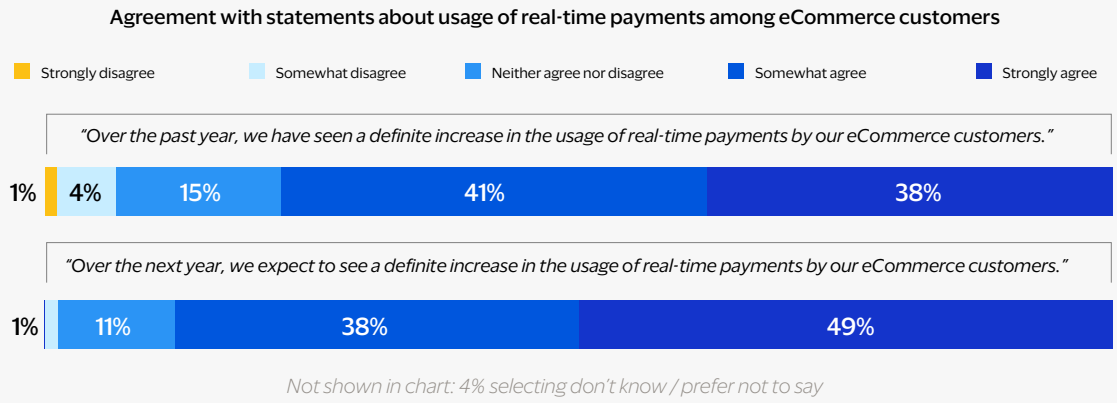
Merchants note a continued increase in real-time payment usage among eCommerce customers

As illustrated by the data in Figure 4 (at the start of this section), roughly four in 10 of merchants (37%) are now accepting RTP which we define as payments made between accounts that are initiated, cleared and settled within seconds and can be completed at any time. Given the industry buzz and increasing adoption of this relatively new payment method, we included additional questions in this year's survey focused specifically on RTP to understand how merchants are seeing customers react to the new offering, as well as whether merchants who do not yet accept RTP are likely to start doing so, in the near future.

Among merchants that do accept RTP, the survey data show 8 in 10 (79%) agree that they have seen a definite increase in the usage of this method by eCommerce customers over the past year, and nearly 9 in 10 (87%) expect to see a marked increase in RTP usage over the next year, as well (see Figure 10). Notably, only 5% of merchants disagree with the first statement, and 1% disagree with the second. These data indicate that merchants that have invested in adding RTP as an acceptance method are seeing strong customer uptake and expect that trend to continue throughout 2025.

Figure 10

Merchant views on customer usage of real-time payments (2025, payment professionals currently accepting RTP)

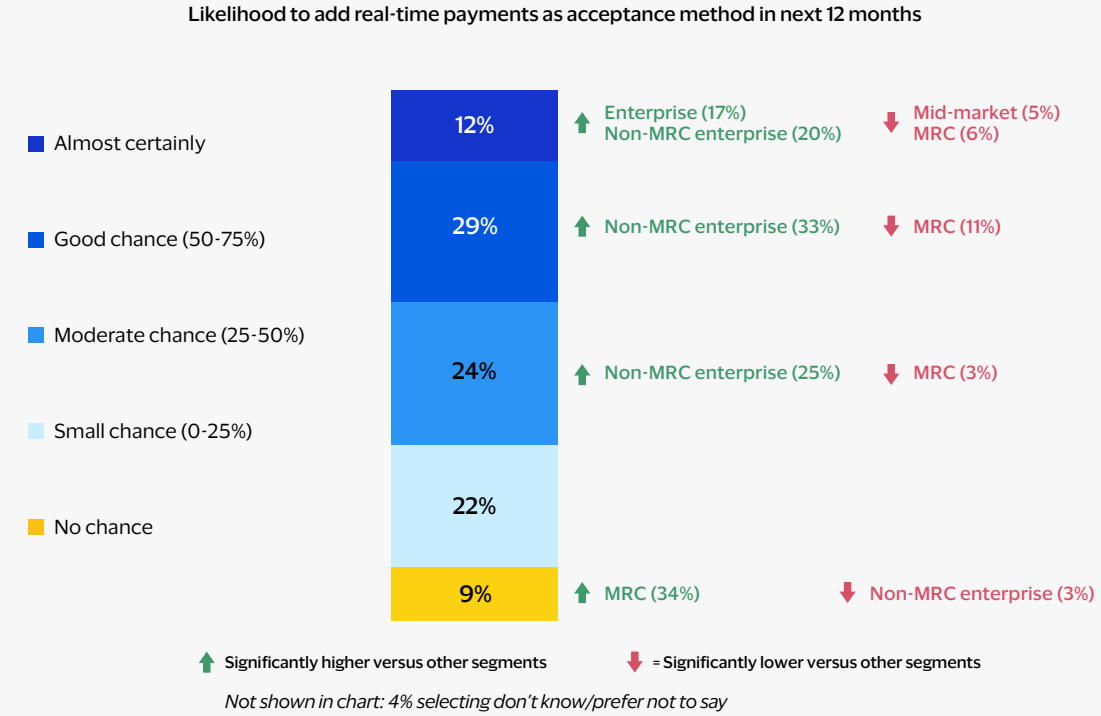


Not shown in chart: 4% selecting don't know / prefer not to say

As for merchants who do not accept RTP, over 4 in 10 (41%) say they are more likely than not to add it as an acceptance method in 2025, with 12% foreseeing this as a near certainty (see Figure 11). In addition, 24% say there is a moderate chance they will add this to their acceptance offering over the next year. Given the claims of growing customer usage (in Figure 10) and strong probability of many more merchants adding RTP acceptance in the coming months, it seems very likely that RTP adoption and implementation will be a major trend in payment acceptance in 2025.

Figure 11

Likelihood to add real-time payments (2025, payment professionals not currently accepting RTP)



Not shown in chart: 4% selecting don't know/prefer not to say

Still, some merchants are taking a wait-and-see approach to RTP. For instance, over one-third of MRC members (34%) say that there is no chance they will add it as an acceptance method in the next year (versus 9% overall). And as with other acceptance methods, mid-market merchants may be slower to adopt RTP than enterprises, given the significant difference in the shares of each who say it is almost certain they will add this method in the next year (5% versus 17%, respectively).

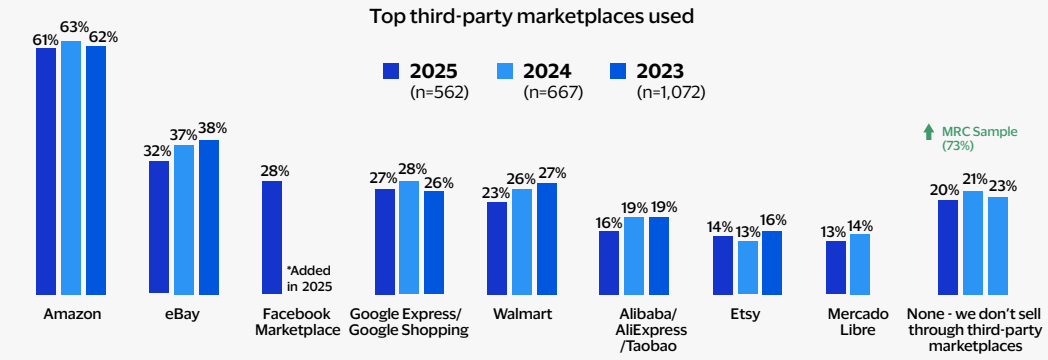
Third-party marketplaces, gateways, and acquirers remain key acceptance partners

Third-party online marketplaces continue to serve as important sales and acceptance partners, especially for midsized merchants. Figure 12 shows the top eight marketplaces used by merchants globally, as well as the main reasons that merchants sell through such marketplaces. Amazon continues to dominate global usage in this space, with over 6 in 10 merchants (61%) selling goods through this site, worldwide. eBay, Facebook Marketplace, and Google Express/Shopping are each used by roughly 3 in 10 merchants, followed by Walmart (23%), Alibaba (16%), Etsy (14%), and Mercado Libre (13%).

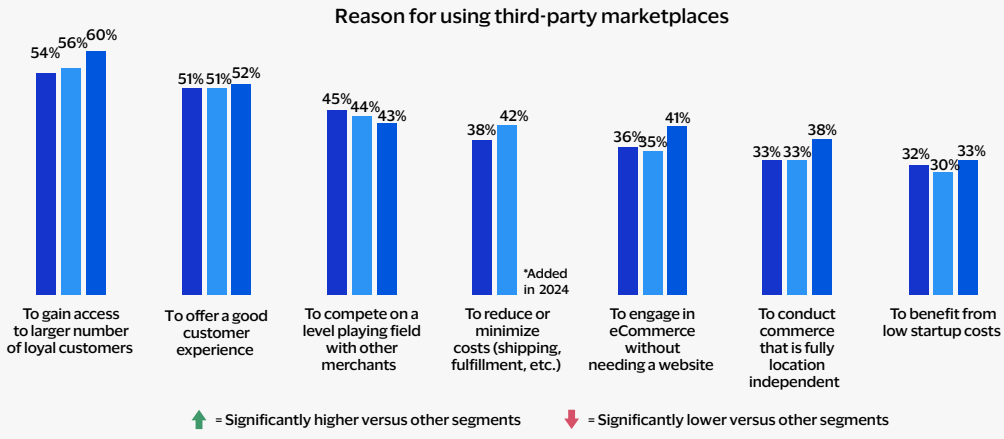
Notably, one in five merchants choose not to sell through any third-party marketplaces, a strategy that is far more prevalent among MRC members than other segments. Nearly three-quarters (73%) of members eschew marketplace partners.

Figure 12

Top third-party marketplaces & reasons for using marketplaces (2023-2025, payment professionals)



*Not shown in chart: Marketplaces used by less than 13% of merchants globally, including Shopee, Booking.com, Target, Rakuten, Temu, Flipkart, Lazada, JD.com, Newegg, Bonanza

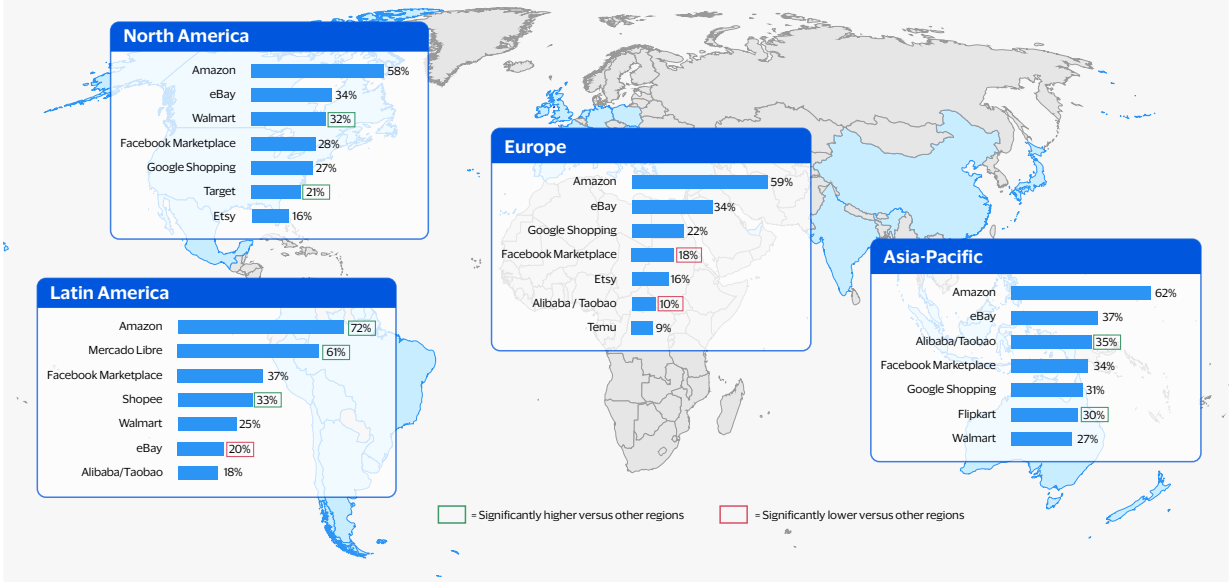


There are good reasons for most merchants to use marketplaces, including their access to larger numbers of loyal customers and their ability to deliver strong customer/shopper experiences (see Figure 12). Competing on a level playing field with larger players and reducing costs are also compelling reasons, as well as the ability to engage in eCommerce without building a website and to conduct commerce that is fully global or location-independent.

Usage of online marketplaces varies dramatically by geographic region. As depicted in Figure 13, North American merchants are more likely to sell through Walmart and Target; those in Latin America skew more heavily toward using Amazon, Mercado Libre, and Shopee; European merchants do not favor any particular marketplace more than those in other regions, but they are significantly less likely to sell on Facebook Marketplace or Alibaba; and merchants in the Asia-Pacific region are more likely to sell their goods and services through Alibaba/Taobao and Flipkart.

Figure 13

Top third-party marketplaces by region (2025, payment professionals)



Marketplace usage also varies significantly by merchant size: 27% of small businesses and 19% of enterprise merchants say they do not sell through any third-party marketplaces, but only 9% of mid-market merchants say the same. Since SMBs may struggle to meet the additional demand from a major marketplace and enterprise merchants may see greater value in directly owning and controlling their sales channels, it makes sense that third-party marketplaces continue to be disproportionately more valuable and important as sales and acceptance partner for midsize merchants (i.e., those generating between $5M and $50M in annual eCommerce revenue).

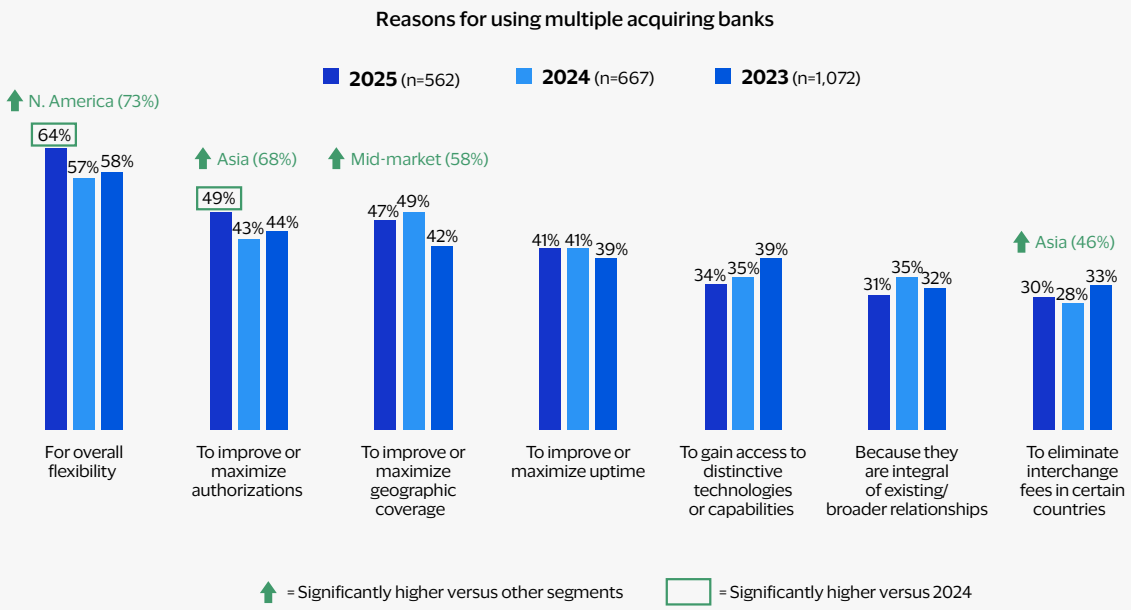
Alongside marketplaces, payment gateways/processors and acquiring banks also serve as critical third-party partners that support payment acceptance for eCommerce merchants. As in previous years, this year's survey shows merchants typically use multiple (three to four, on average) payment gateways and acquiring banks. Merchants in Latin America use more payment gateways or processors compared to those in North America, while merchants in Asia Pacific tend to use more merchant acquiring banks than those in North America and Europe. SMBs use fewer partners in both categories, than midsize and enterprise merchants. And non-MRC enterprises support significantly more gateway or processor connections than MRC members.

Figure 14

Numbers of gateways and acquirers used and top reasons for using multiple acquirers (2023-2025, payment professionals)

Avg. number of payment partners used	2025	By region				By size			By membership	
		North America	Europe	Asia-Pacific	Latin America	SMB	Mid-market	Enterprise	MRC sample	Non-MRC enterprises
# of payment gateway or processor connections currently supported	3.9	3.6 (3.7)	3.8 (4.2)	4.1 (4.4)	4.5 (4.3)	3.4 (3.5)	4.0 (4.4)	4.1 (4.3)	3.1 (3.5)	4.3 (4.5)
# of merchant acquiring banks currently used	3.2	3.0 (3.0)	2.9 (3.6)	3.7 (3.7)	3.5 (3.9)	2.6 (2.9)	3.1 (3.6)	3.4 (3.7)	3.1 (3.3)	3.5 (3.8)

= Significantly higher versus other segments = Significantly lower versus other segments (xx%) = 2024 figures



Compared with last year, merchants are far more likely to seek multiple acquirer partners to maximize overall payment flexibility and authorization rates (see Figure 14). Having multiple acquirer partners also provides increased geographic coverage, which is especially valuable for mid-market merchants. And for merchants in Asia, additional acquirer partners can offer ways to avoid Interchange fees they may deal with when accepting or processing payments in certain countries.

2. Payment metrics and tactics

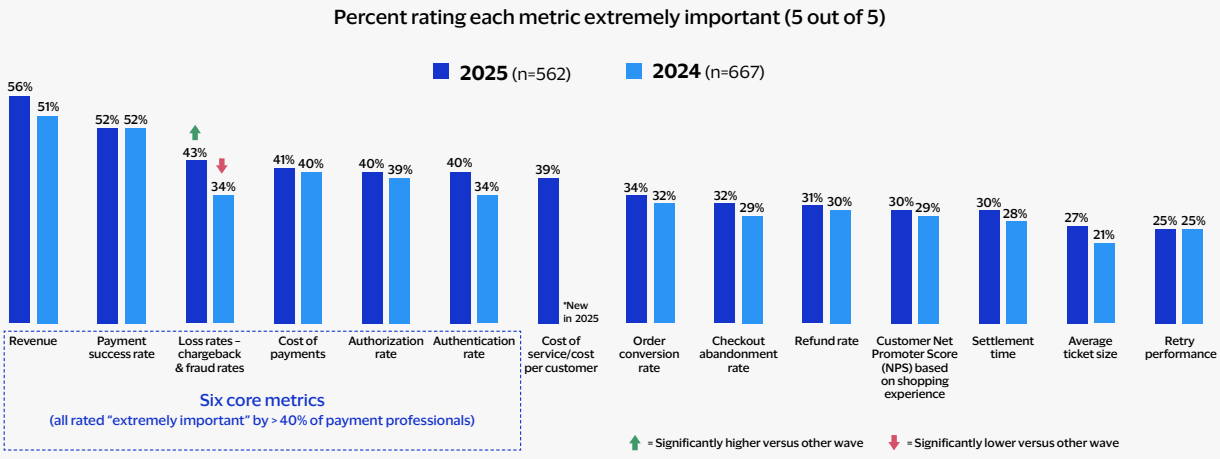
In this section, the focus shifts from payment acceptance to payment metrics and tactics. This includes topics like which payment metrics or KPIs are considered most important, how and why merchants employ tokenization, and what kinds of techniques merchants use to increase or maximize authorizations on their accepted payment transactions.

All payment management metrics tested are uniformly considered important

Out of 14 payment metrics tested in the survey, every single metric was rated "very or extremely important" by over half of all payment professionals taking part. In other words, merchants should see at least some value in measuring and analyzing all of the metrics covered here, if possible. But within this large set of metrics, there are six that stand out as "extremely important" to at least 4 in 10: revenue, success rate, loss rate, authentication rate, authorization rate, and cost of payments (see Figure 15). Within this "core" set of payment indicators, loss rate is notable, as its importance has grown significantly over the past year.

Figure 15

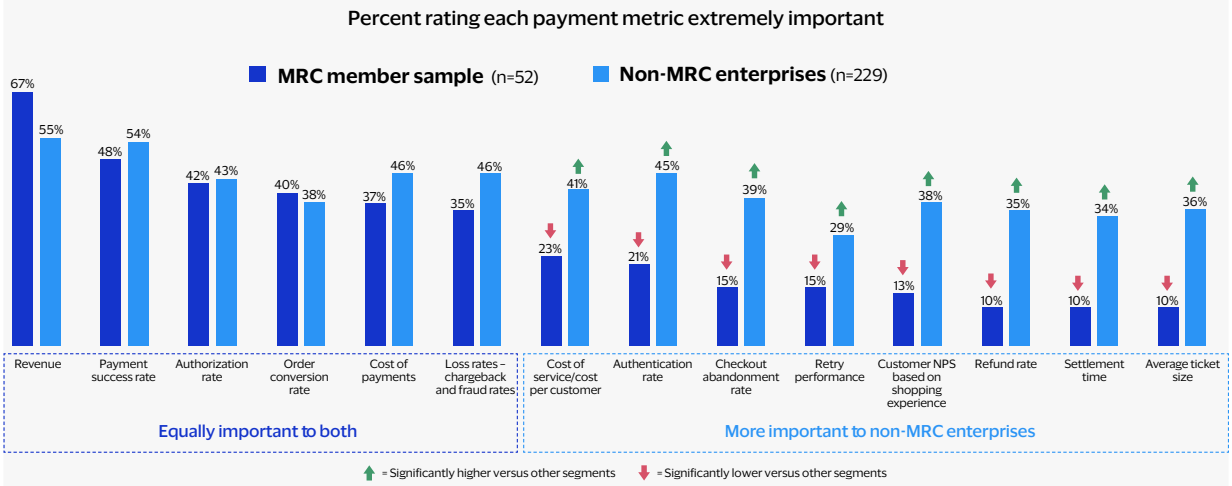
Importance of payment metrics (2024-2025, payment professionals)



The metrics considered most important are consistent across regions and size segments, but there is a stark difference in the views of MRC members and non-MRC enterprises on this subject. Both groups are equally likely to rate the "core" six indicators extremely important, however MRC members are far less likely to view all the other metrics tested in the survey as extremely important. This difference is vividly illustrated by the chart in Figure 16.

Figure 16

Importance of payment metrics by MRC membership (2024-2025, payment professionals)



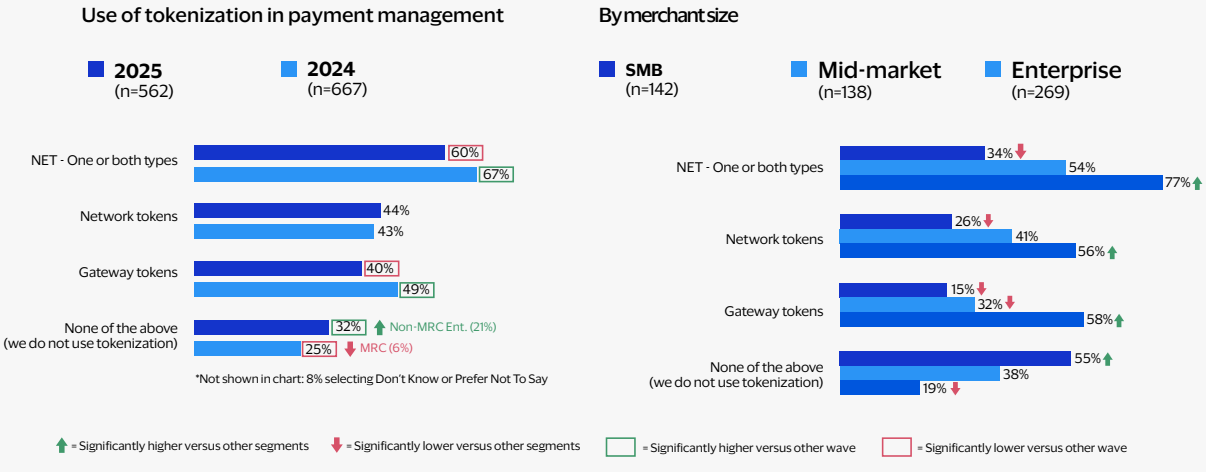
Usage of payment tokenization declines, driven by shift away from gateway tokens

Globally, 6 in 10 merchants (60%) use tokenization in payments, with a slight decrease compared with 2024 (see Figure 17). While usage of network tokens has remained steady, usage of gateway tokens has declined significantly, from 49% to 40%.

Data also shows an increase in network tokens. And as noted in the left-hand chart in Figure 17, MRC members are far more likely to still be employing some form of tokenization compared with non-MRC enterprises. Tokenization tactics also vary significantly by merchant size, with mid-market and enterprise merchants generally far more likely than SMBs to use either network and/or gateway tokens.

Figure 17

Usage of payment tokenization overall and by merchant size (2024-2025, payment professionals)



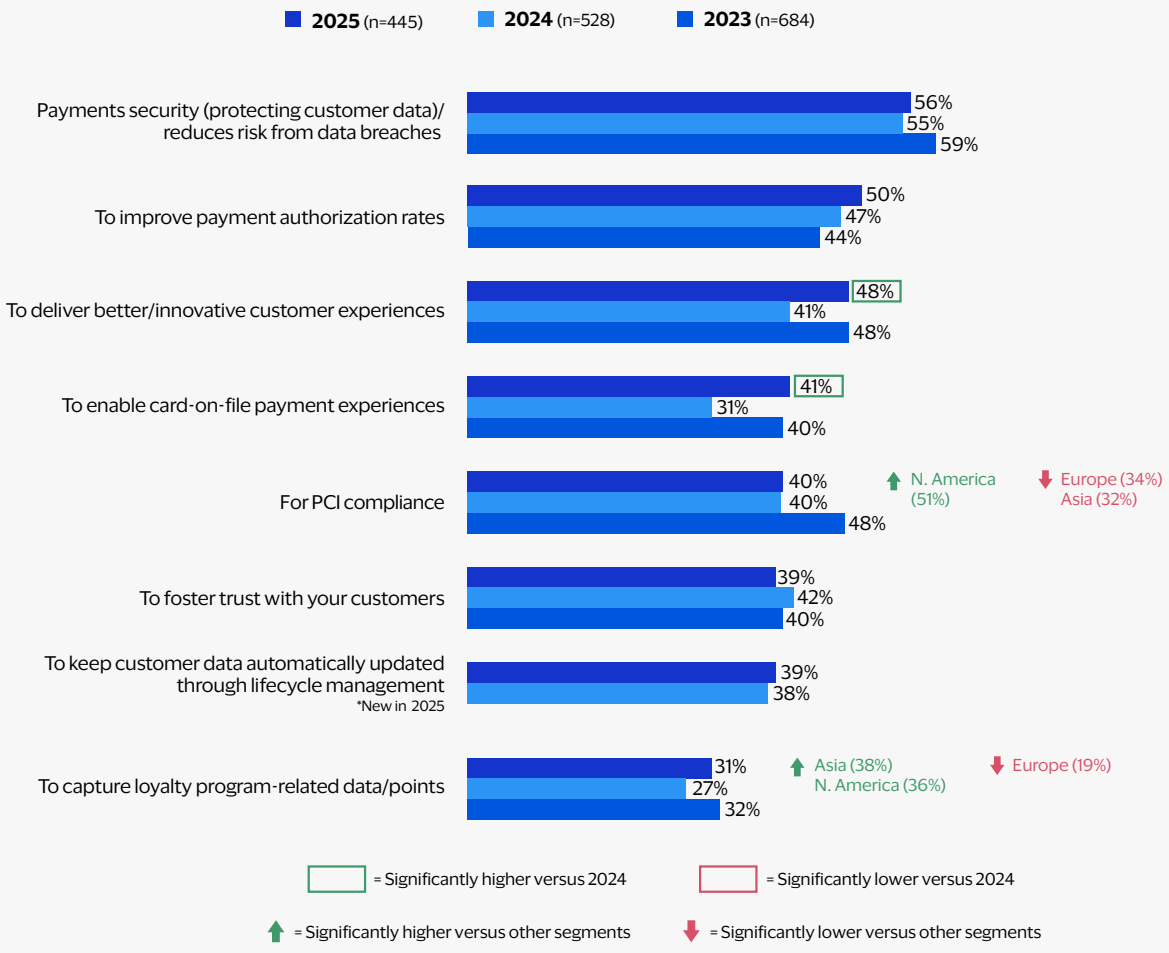
Protecting customer data and reducing risk from data breaches remain the top reasons for using tokenization

Most merchants (60%) still employ tokenization and, as shown in Figure 18, they have several good reasons for doing so. The most commonly cited benefits of tokenization include payments security/reduced risk of data breaches, improved payment authorization rates, enhanced customer experiences and the ability to enable card-on-file payment experiences (note: the share of merchants citing the latter two benefits increased significantly in this year's survey).

Other benefits include ensuring Payment Card Industry Data Security Standards (PCI DSS) compliance (significantly more important to merchants in North America versus those in Europe and Asia), fostering trust with customers, and keeping customer data automatically updated through lifecycle management, as well as capturing loyalty program data (more important to North American and Asian merchants versus those in Europe).

Figure 18

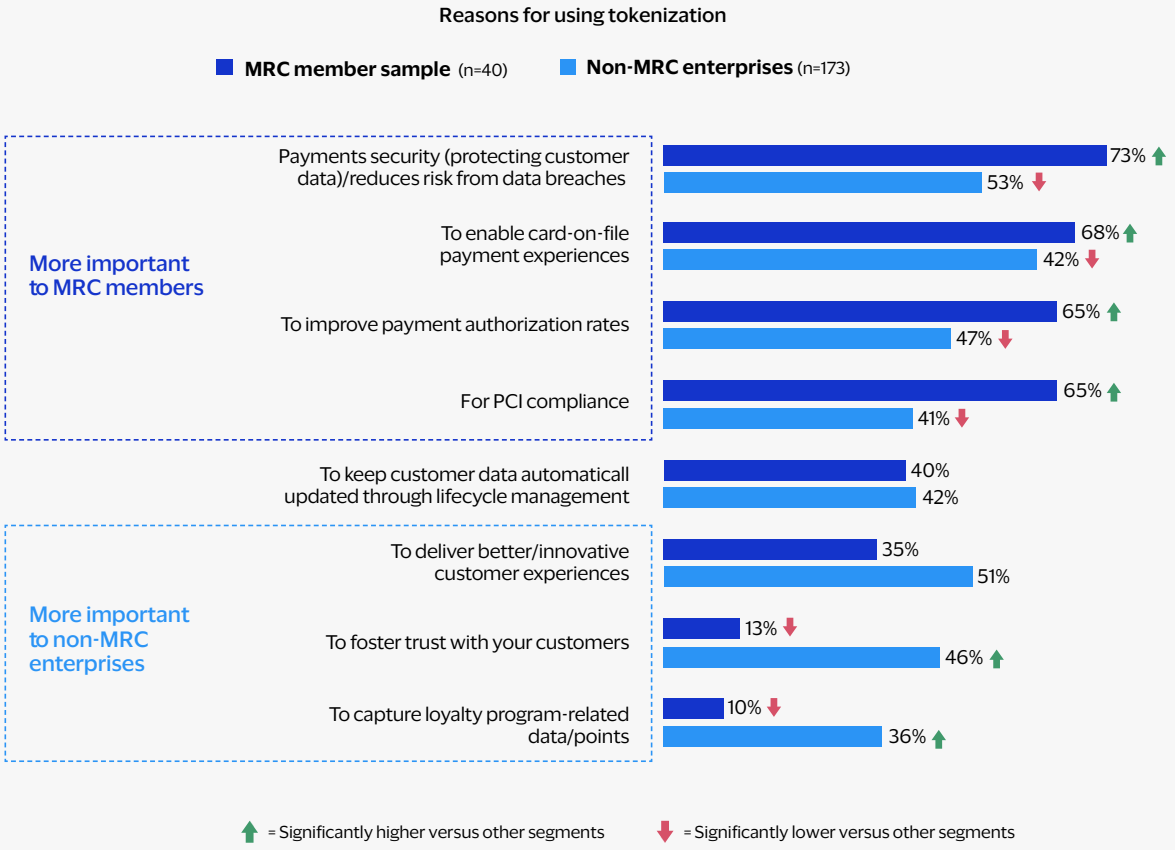
Reasons for using tokenization (2023-2025, payment professionals using tokenization)



MRC members, and non-member enterprises differ quite a bit in their reasoning for using tokenization (see Figure 19). MRC members are far more likely to see tokenization's main benefits as increased payments security/reduced risk of data breaches, enablement of card-on-file payment experiences, improvement in payment authorization rates and increased certainty around maintaining PCI DSS compliance. Many non-MRC enterprises also cite these as important benefits, but they are also significantly more likely than MRC members to call out additional reasons for employing this tactic, including delivering better customer experiences, fostering trust with customers and capturing loyalty program-related data.

Figure 19

Reasons for using tokenization by MRC membership (2025, payments professionals using tokenization)



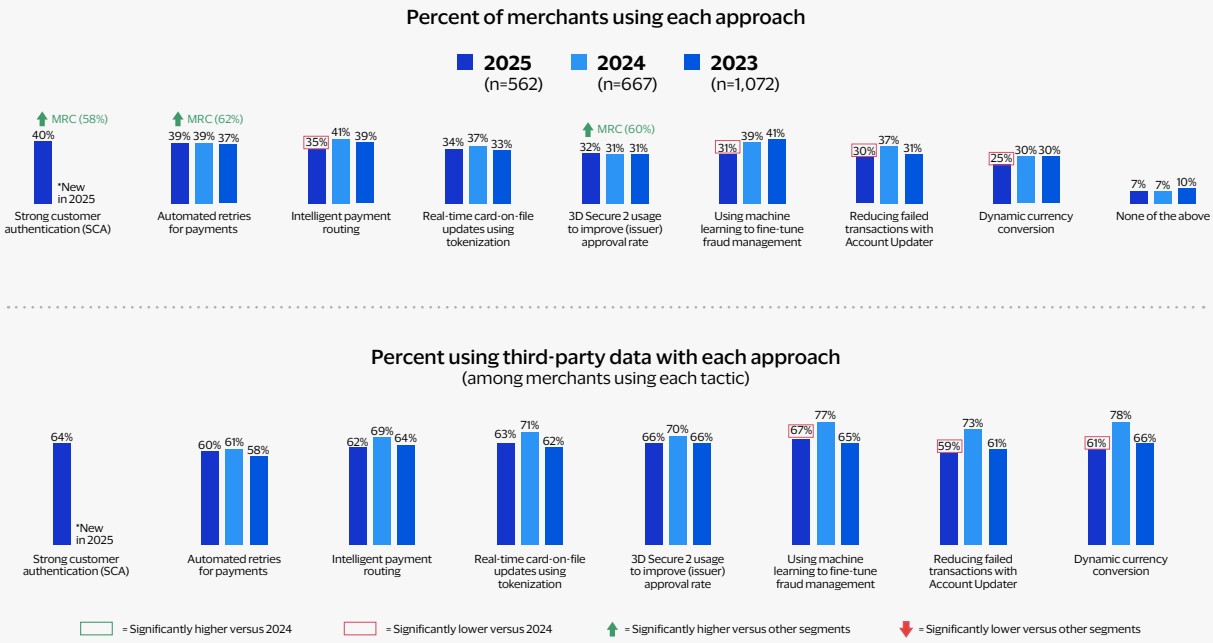
Strong customer authentication (SCA) and automatic retries are the two most common authorization tactics utilized

Concluding this final section on eCommerce payments are fresh insights uncovered by this year's survey on the tactics merchants use to maintain and maximize authorization rates. Over 90% of merchants report using at least one authorization-related tactic shown in Figure 20, but there is no "silver bullet" to be found here, as usage rates for all tactics are fairly similar, ranging from 40% for SCA down to 25% for dynamic currency conversion (see Figure 20). There is some indication that certain tactics may be falling out of favor with merchants, as usage rates for intelligent payment routing, using ML to fine-tune fraud management, reducing failed transactions with Account Updater and dynamic currency conversion all declined significantly this year, compared to 2024.

Utilization of authorization-related approaches tends to vary by segment. Enterprises are significantly more likely than SMBs to use virtually all of these methods, while MRC members over-index on usage of SCA, automated retries, and 3D Secure 2.0, compared with their peer group of non-MRC enterprises.

Figure 20

Usage of authorization tactics and usage of third-party data to support them (2023-2025, payment professionals)



3. Fraud attacks and metrics

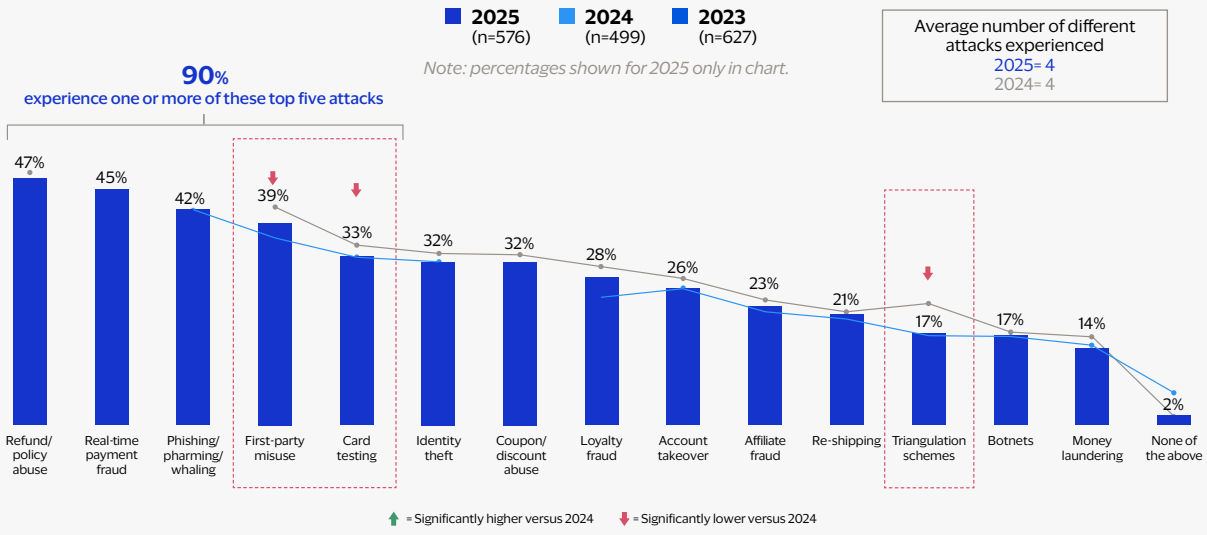
The three remaining sections of this report focus on topics and trends related to eCommerce fraud. This section examines insights regarding the kinds of fraud attacks merchants are experiencing, as well as the impacts of fraud on merchant businesses, as measured through various key metrics and indicators.

Fraud rates are down, with significant declines in first-party misuse, card testing, and triangulation schemes

Fraud remains a universal challenge, with 98% of merchants experiencing one or more types of fraud in the past 12 months. Yet this year's survey data show a slight but consistent decline in incidence of virtual forms of fraud, as well as significant declines in the shares of merchants impacted by first-party misuse, card testing, and triangulation schemes (see Figure 21).

Figure 21

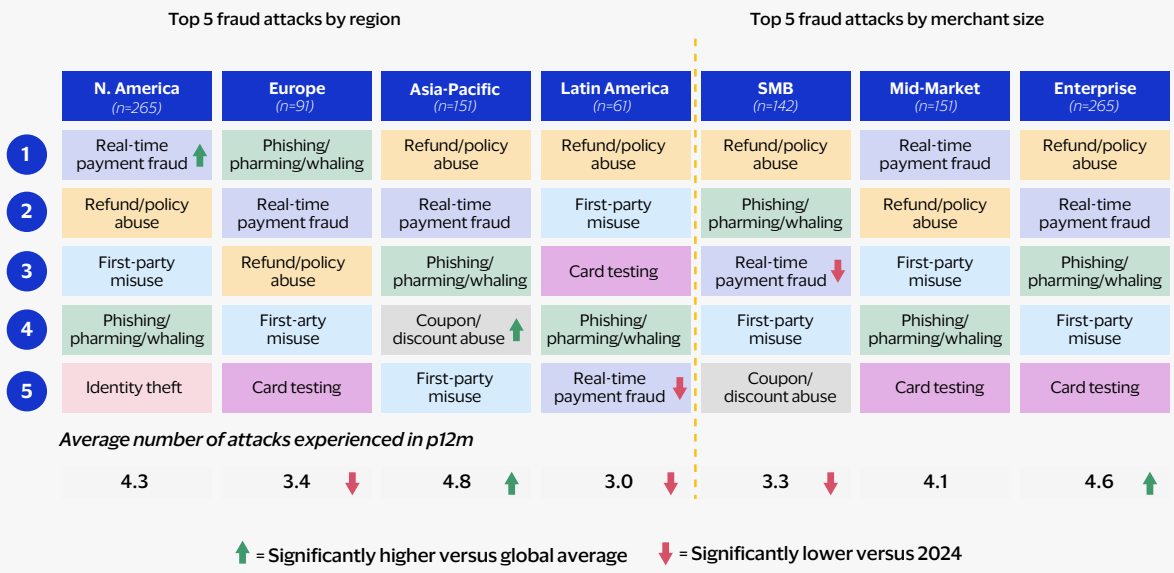
Types of fraud experienced in past 12 months (2023-2025, fraud professionals)



The decline in first-party misuse is especially noteworthy, given that our surveys over the past two years have shown the incidence of this type of fraud rising rapidly. Also notable is the emergence of real-time payment RTP fraud as the second most widespread fraud attack, overall, impacting 45% of merchants globally. Along with RTP fraud, the most widespread attacks continue to be refund/policy abuse, phishing/pharming/whaling, first-party misuse and card testing, all impacting between 33% and 47% of merchants over the past year.

Figure 22

Top five fraud attacks experienced in past 12 months by region & size segment (2025, fraud professionals)



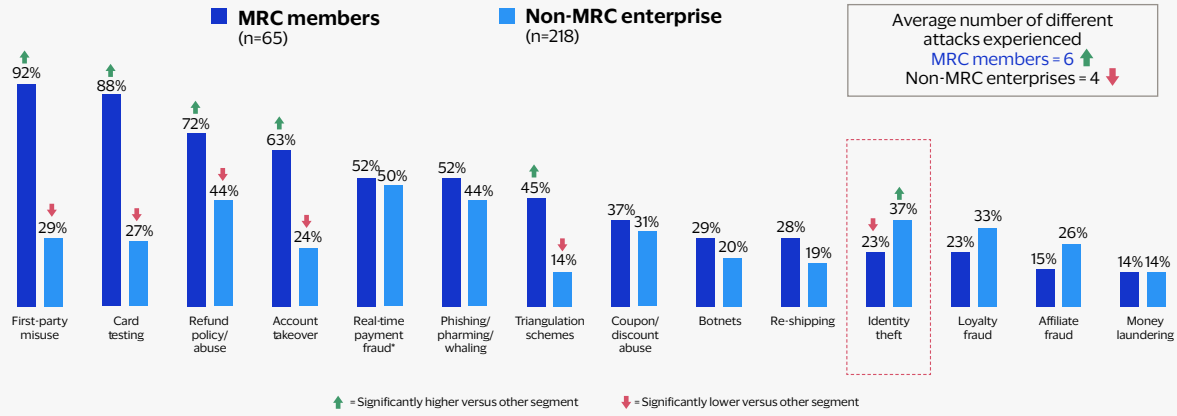
There are some differences by region and by company size, when it comes to the most prevalent types of fraud impacting merchants (see Figure 22). For instance, North American merchants are significantly more likely to suffer RTP fraud, while those in Latin America are significantly less likely. Small businesses are less likely than midsize and enterprise merchants to experience RTP fraud. And merchants in Asia are more likely than average to face coupon/ discount abuse.

As indicated by the numbers near the bottom of Figure 22, there are also some differences in the variety of attacks faced by merchants in different regions and size segments. Merchants in Asia experience a wider range of fraud attacks than average, while those in Europe and Latin America are impacted by a significantly narrower range of threats. Similarly, enterprise merchants face a wider variety of different fraud attempts, while SMBs under-index in this regard.

As in previous years, MRC members continue to grapple with greater variety and volume of fraud attacks compared with non-MRC enterprises (see Figure 23). The average MRC merchant experienced six attacks in the past year, compared with four for the average non-MRC enterprise. In particular, MRC members are significantly more likely to suffer first-party misuse, card testing, refund/policy abuse, account takeover, and triangulation scheme attacks. The only form of fraud that non-MRC enterprises experience at higher rates is identity theft, which impacts nearly 40% of that group, versus 23% of MRC members.

Figure 23

Fraud attacks experienced in past 12 months by MRC membership (2025, fraud professionals)



It is important to understand that the stark differences in fraud incidence between MRC members and non-members may be driven by 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 41). So, MRC members may also 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 also show slight improvement

In addition to declining incidence for all forms of fraud, fraud professionals in this year's survey reported slight improvement in a range of other fraud-related metrics. In particular, order rejection rates declined significantly from 5.8% to 5.0% globally. Fraud rate by order also dipped somewhat, falling from 3.4% to 3.0% overall (see Figure 24). Average fraud rate by revenue and chargeback/dispute win rate remained statistically consistent with the rates reported last year.

Figure 24

Fraud-related metrics (2024-2025, fraud professionals)

Fraud-related metrics *(Trimmed averages shown)*	Overall		By region				By size			MRC members	
	2024	2025	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)	3.1%	**3.2%**	3.6% (2.8)	2.8% (3.5)	2.6% (3.3)	4.1%* (2.7) *Low Base Size	3.4% (3.7)	3.2% (4.1)	3.3% (2.3)	0.5% (0.6)	4.4% (3.9)
Fraud rate by order (% accepted orders in past 12 months that turned out to be fraudulent)	3.3%	**3.0%**	3.4% (3.6)	2.8% (2.8)	2.5% (3.6)	3.9% (3.4*)	3.4% (4.3)	3.0% (3.7)	3.1% (2.6)	0.4% (0.6)	4.0% (4.0)
Order rejection rate (% eCommerce orders rejected due to suspicion of fraud in past 12 months)	5.8%	**5.0%**	5.2% (6.5)	5.2% (4.3)	4.5% (5.5)	5.9% (6.0)	5.0% (6.2)	4.6% (5.1)	5.4% (5.9)	2.5% (3.3)	6.2% (7.5)
Chargeback / dispute win rate (annual % of fraud-coded chargebacks & disputes won by the merchant)	17.4%	**17.1%**	17.9% (20.8)	15.1% (10.3)	19.6% (15.6)	11.5% (16.6)	18.2% (16.6)	17.0% (15.0)	16.4% (18.8)	27.2% (28.0)	15.0% (16.0)

= Significantly higher versus other segments = Significantly lower versus other segments (% = 2024 figures) (Significantly higher versus 2024) (Significantly lower versus 2025)

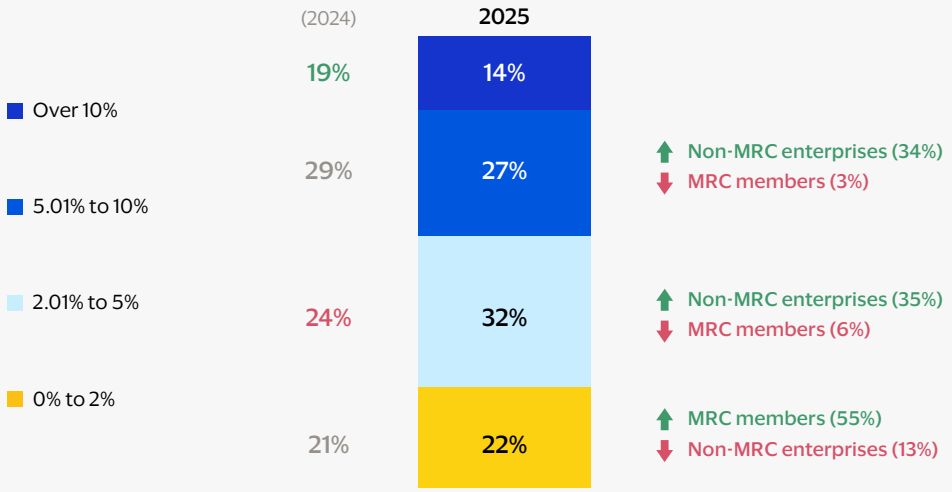
There are also significant differences by region and MRC membership on these indicators: Merchants in the Asia-Pacific region report significantly lower fraud rates by revenue and by order compared with those in North and Latin America. Merchants in Asia and North America also report significantly higher win rates than those in Latin America.

And continuing a multi-year trend, we see fraud metrics for MRC members looking significantly stronger than those for non-MRC enterprises, with fraud rates by revenue and by order around 10 times lower for MRC members, order rejection rates over two times lower, and chargeback/dispute win rates nearly two times higher for MRC merchants versus non-members (see Figure 24). 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.

In addition to the impacts quantified in Figure 24, fraud also frays merchant relationships with both 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 that they believe to be fraudulent. Figure 25 shows that around 6 out of 10 merchants cite false positive rates between 2% and 10% of disputed eCommerce orders.

Figure 25

Rate of false positives or "customer insults" (2024-2025, fraud professionals)



*Not shown in chart: 5% selecting don't know or prefer not to say

= Significantly higher versus other segments

= Significantly lower versus other segments

Last year, our survey showed nearly 1 in 5 merchants skewing significantly higher than this range, reporting false positive rates above 10%. But this year, it seems merchants have made some progress in this regard, as the share reporting false positive rates over 10% declined significantly to just 14% of merchants globally. Instead, there are significantly more merchants in this year's survey reporting low-to-average rates, falling in the 2-5% range (32%, compared to 24% last year). Here, too, MRC members are outperforming their non-MRC enterprise peers by a considerable margin: While the majority of MRC members (55%) report false positive rates of 2% or less, most non-MRC enterprises (69%) report rates over 2%, and only 13% are able to claim the same low customer insult rates as those reported by most members of the MRC.

In general, the survey data reflect a slightly but consistently positive story for merchants, as they continue to grapple with the challenging and fast-changing constellation of fraud attacks and impacts they face in today's eCommerce marketplace. Fraud rates are ticking down, and merchants are having greater success preventing and mitigating fraud-related harms to both their businesses and their customers. But fraud remains a universal concern, impacting essentially every eCommerce merchant in every region and category/vertical. As indicated by the data and trends discussed in the following section, even when gaining back some ground in this fight, merchants cannot afford to become complacent, as they are sure to face new threats and impacts driven by fraudsters in the near future.

Post-purchase fraud and abuse

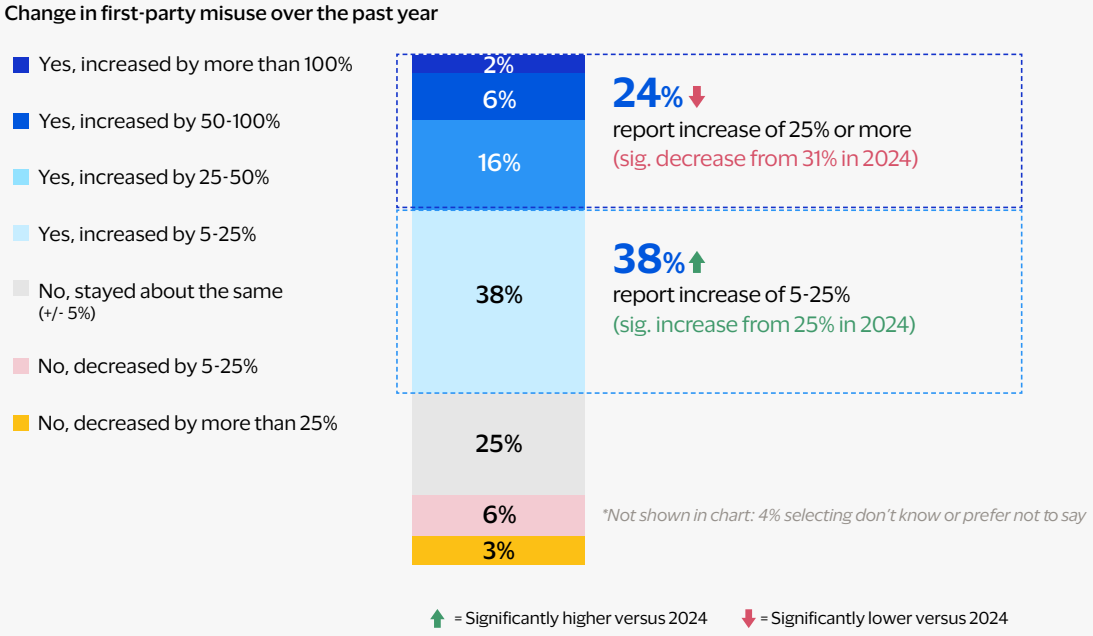
Over the past two years, our research has revealed a steady and significant increase in various types of post-purchase fraud and abuse. Issues like FPM, chargeback fraud, and refund/policy abuse have become more widespread and more damaging, both to merchant businesses and to the issuers, acquirers, and other payment partners that support eCommerce transactions. This year, our survey again delves into the salient problem of post-purchase fraud focusing, in particular, on merchants' experiences and opinions regarding FPM and refund/policy abuse.

Merchants see a slowdown in first-party misuse, shift more blame to consumers and issuers

When we asked all survey respondents (both fraud and payment professionals) to estimate the change in first-party misuse over the past year, the results tell an encouraging story: Similar to last year, 62% of merchants claim FPM rose by at least 5% over the past year (see Figure 26).

Figure 26

Change in first-party misuse over the past year (2025, fraud and payment professionals)



But within that majority, this year's survey shows significantly fewer merchants claiming a major increase of 25% or more (24%, versus 31% last year), and significantly more merchants reporting a smaller uptick of 5% to 25% (38%, versus 25% last year). Overall, these data points indicate that while FPM remains a major issue impacting a large share of merchants each year, its momentum has slowed significantly.

FPM affects some types of merchants significantly more than others. Mid-market and enterprise merchants are significantly more likely to continue seeing increases in FPM, compared with small businesses (see Figure 27). And non-MRC enterprises are more likely to cite continued increases than MRC members. For merchants in these segments, additional focus, effort, and investment may be required to continue to stem the tide of FPM over the coming years.

Figure 27

Change in first party-misuse by region, size segment & MRC membership (2025)

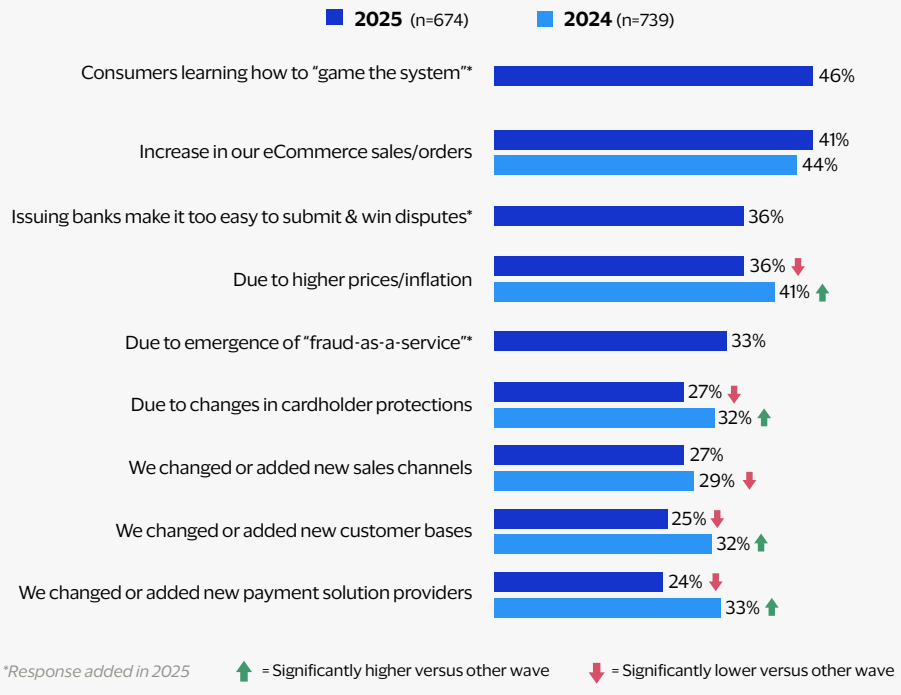
Change in first-party misuse over the past year	2025	Region				Merchant size			Membership	
	Overall	North America	Europe	Asia-Pacific	Latin America	SMB	Mid-Market	Enterprise	MRC sample	Non-MRC enterprises
Base	1,082	447	219	255	153	284	285	495	70	443
Net % citing any increase	**62%**	**61%**	**61%**	**68%**	**60%**	**49%**	**67%**	**68%**	**51%**	**70%**
Yes, increased by more than 100%	**2%**	1%	2%	2%	2%	2%	1%	2%	0%	2%
Yes, increased by 50-100%	**6%**	6%	5%	6%	7%	4%	5%	8%	7%	8%
Yes, increased by 25-50%	**16%**	16%	16%	20%	12%	14%	18%	18%	11%	18%
Yes, increased by 5-25%	**38%**	38%	38%	39%	39%	29%	44%	41%	33%	42%
No, stayed about the same (+/- 5%)	**25%**	28%	28%	17%	27%	37%	20%	22%	24%	21%
No, decreased by more than 25%	**9%**	7%	7%	13%	11%	9%	11%	8%	10%	8%
Don't know / we do not track OR Prefer not to say	**4%**	4%	4%	3%	2%	5%	1%	1%	15%	1%

= Significantly higher versus 2024 = Significantly lower versus 2024

As the spike in FPM slackens, merchants also sense a shift in the underlying drivers that cause this form of fraud to increase. Last year, the top reasons merchants cited for rising FPM were fundamentally economic in nature: increasing eCommerce sales and higher prices/inflation. This year, merchants are more likely to point to consumers learning how to "game the system" as well as issuers making it too easy for consumers to submit and win fraudulent disputes (see Figure 28). Along with these two factors, increasing eCommerce sales continue to be linked to rising FPM by around 4 in 10 merchants globally.

Figure 28

Reasons why FPM Is increasing (2024-2025, fraud and payment professionals)

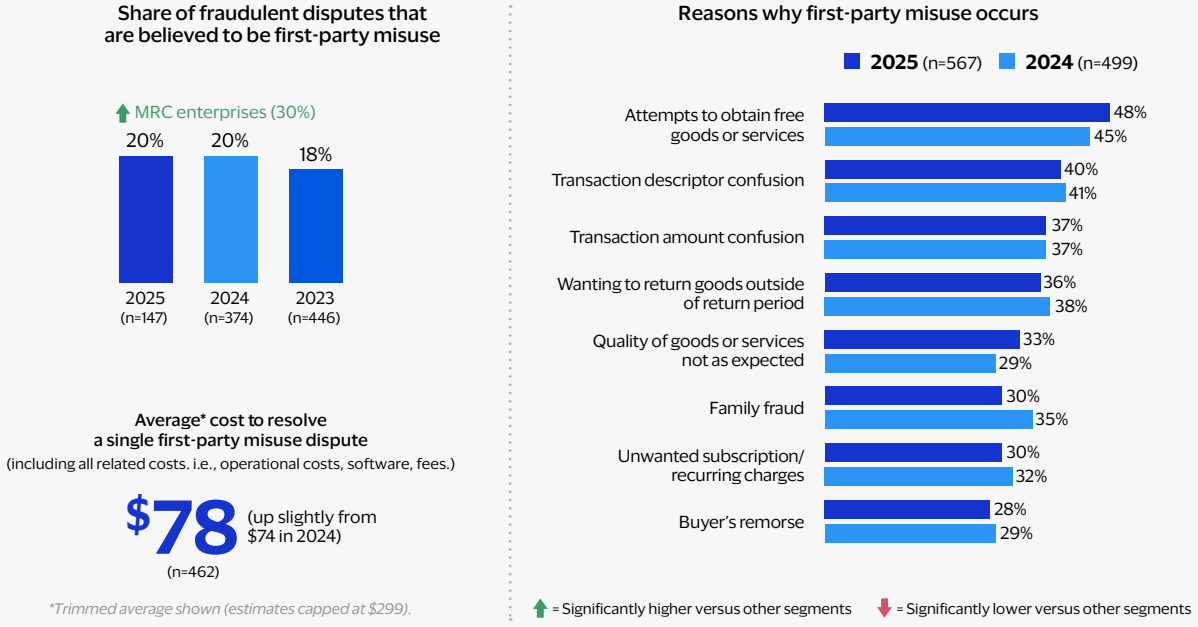


Compared with last year, significantly fewer merchants ascribe rising FPM to inflation or to changes in cardholder protections, customers bases, or payment solution providers. In fact, while less than 3 in 10 merchants cite any of those three factors, one-third attribute rising FPM to the emergence of "fraud-as-a-service" – a concerning development that may contribute to increases in other forms of fraud.

While the results above paint a somewhat encouraging picture of FPM having a less harmful impact on many merchants over the past year, the fact remains that it still accounts for a sizable share of fraudulent disputes, and it continues to have significant financial impacts on merchant organizations, which must invest significant time, talent, and money in preventing and mitigating FPM disputes. Figure 29 shows that the estimated share of all fraudulent disputes that merchants attribute to FPM remains consistent with last year, at 20%. And for MRC members, this share skews significantly higher, up to 30%.

Figure 29

Drivers of FPM, share of fraudulent disputes, and costs to resolve disputes (2023-2025, fraud professionals)

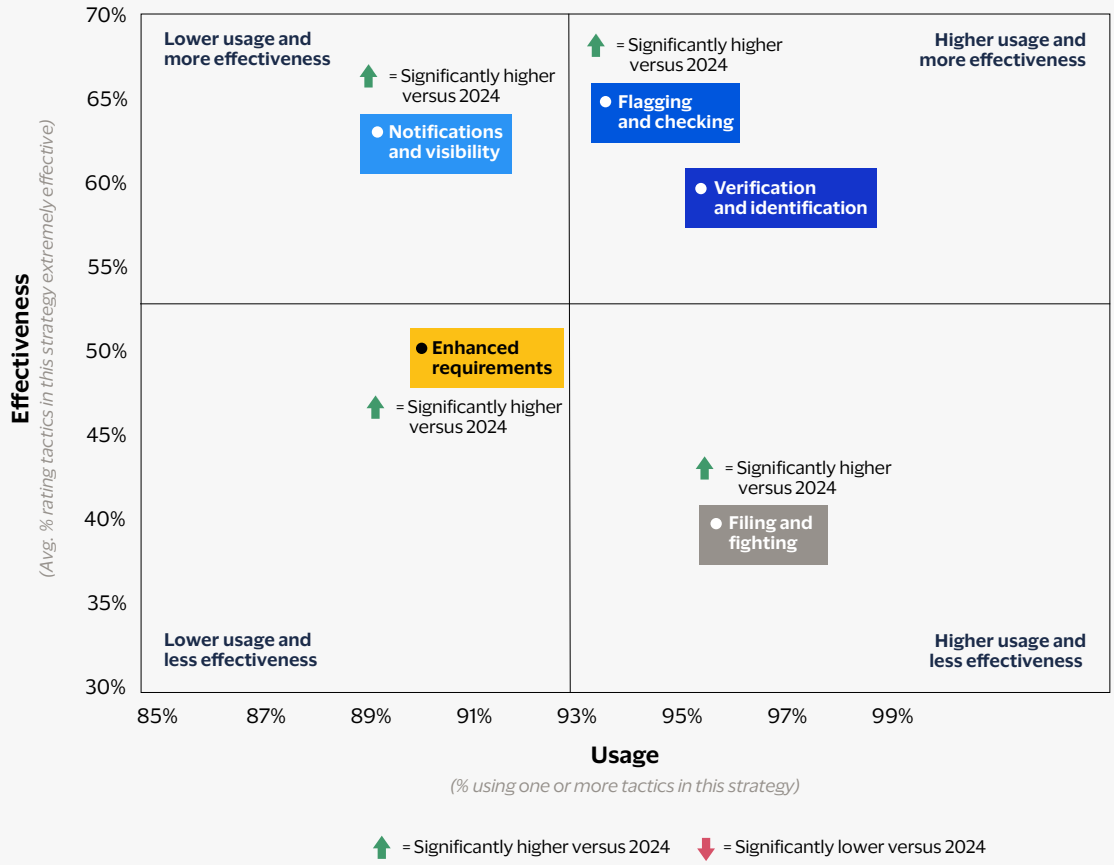


Meanwhile, the average cost to resolve each of those disputes ticked upward, from $74 to $78, this year. And while the reasons for rising FPM shifted a bit over the past year (as shown in Figure 28), the basic underlying causes of this form of fraud remain quite consistent: Merchants continue to point to attempts to obtain free goods or services, transaction descriptor or amount confusion, and attempts to return goods outside of the return period as the primary reasons why FPM occurs in the first place.

With FPM still ticking upward for some merchants and driving a sizable share of disputes and dispute-related costs, is the merchant community making measurable progress in combating this thorny issue? Our data indicates they are. At the strategic level, merchants utilize five different approaches to combat FPM. Figure 30 shows these five approaches mapped by usage (on the x-axis) and by perceived effectiveness (on the y-axis). As indicated by the relatively close clustering of all five approaches on the x-axis, each strategy is being used by around 90% of merchants, worldwide. In other words, merchants are generally pulling all of the strategic levers they have available in their efforts to quash the problem of FPM. And with these usage rates remaining statistically consistent, year-over-year it's clear there is little headroom to achieve further gains in the fight against FPM through increased adoption of any of these strategic approaches.

Figure 30

Usage vs. effectiveness of strategies for combating first-party misuse (2025, fraud professionals)



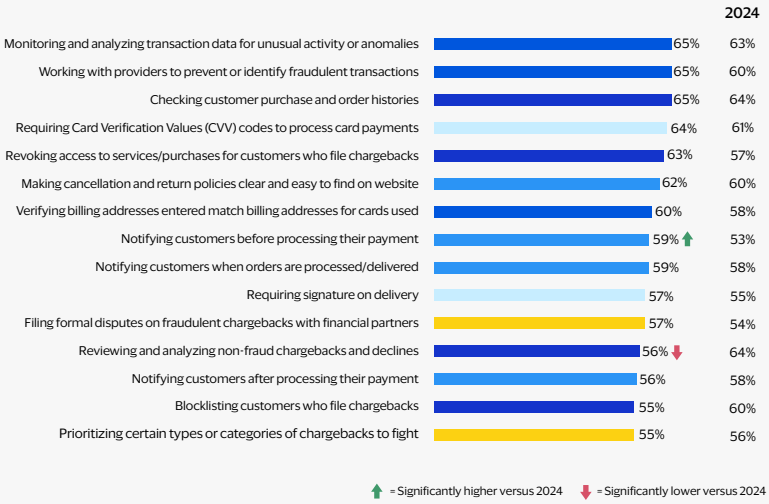
But where there is more differentiation — and much more room for improvement — is on the y-axis of this chart, indicating the relative effectiveness of each strategy. And indeed, merchants are making significant advances in ramping up the impact of their anti-FPM efforts, as the effectiveness ratings of all five strategies rose significantly in this year's survey. In short, merchants are not only pulling out all the stops to fight FPM; they are seeing those efforts bear greater fruit in reducing this problem over time.

Drilling down from the high-level, strategic approaches merchants use to combat FPM, what specific tactics, tools and techniques do they employ when implementing these strategies day-to-day? This information is detailed in Figure 31. Four of the top five most effective tactics involve either verification and identification or flagging and checking. These include monitoring transaction data for anomalies, working with providers to prevent or flag fraudulent transactions, checking customer purchase and order histories, and revoking access to services/purchases for customers who file chargebacks. Requiring Card Verification Value (CVV) codes to process card payments — a tactic within the enhanced requirements strategy — rounds out the top five.

Figure 31

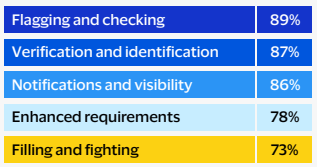
Effectiveness of strategies and tactics to combat first-party misuse

(% using each tactic rating it as very or extremely effective)



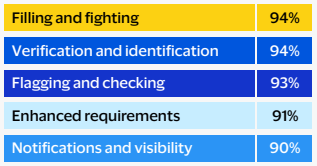
Effectiveness of anti-FPM strategies

(% rating at least one tactic in each group as very or extremely effective)



Usage of anti-FPM strategies

(% using one or more tactics in each grouping)

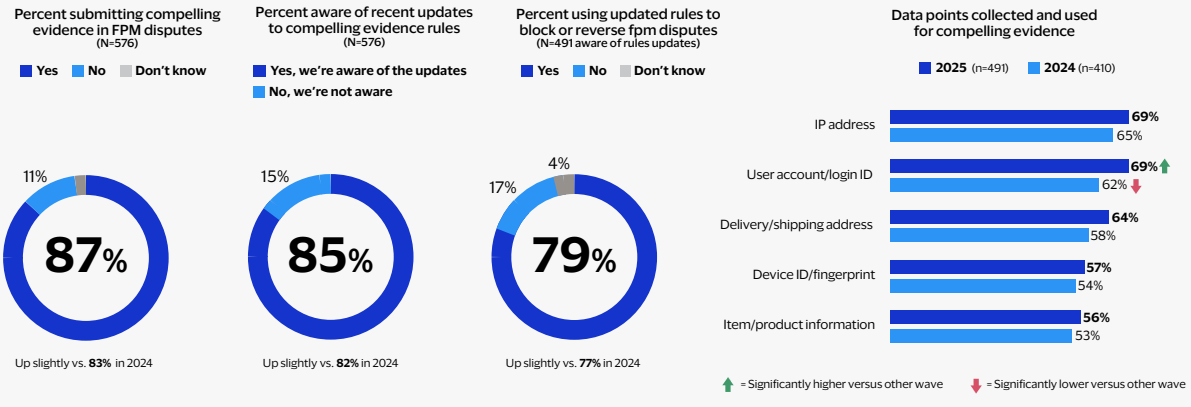


While the effectiveness of most tactics has stayed consistent over time, there were two notable shifts captured in this year's survey: Significantly more merchants are finding notifying customers before processing their payment to be more effective this year, while significantly fewer merchants say the same about reviewing and analyzing non-fraud chargebacks and declines. Overall, these data offer useful benchmarks and guidance for merchants seeking to make further progress in the battle against first-party misuse.

In addition to ramping up the effectiveness of anti-FPM tactics, merchants are also making progress against this form of fraud by increasingly embracing and leveraging the compelling evidence rules and processes set forth by the major card networks. The share of merchants who are submitting compelling evidence and keeping up to date on card brands' updates to these rules increased slightly in this year's survey. And merchants are using more of the relevant data points that are accepted as compelling evidence, with significantly more merchants sharing user account/login ID information, in particular.

Figure 32

Awareness and usage of compelling evidence in FPM disputes (2024-2025, fraud professionals)

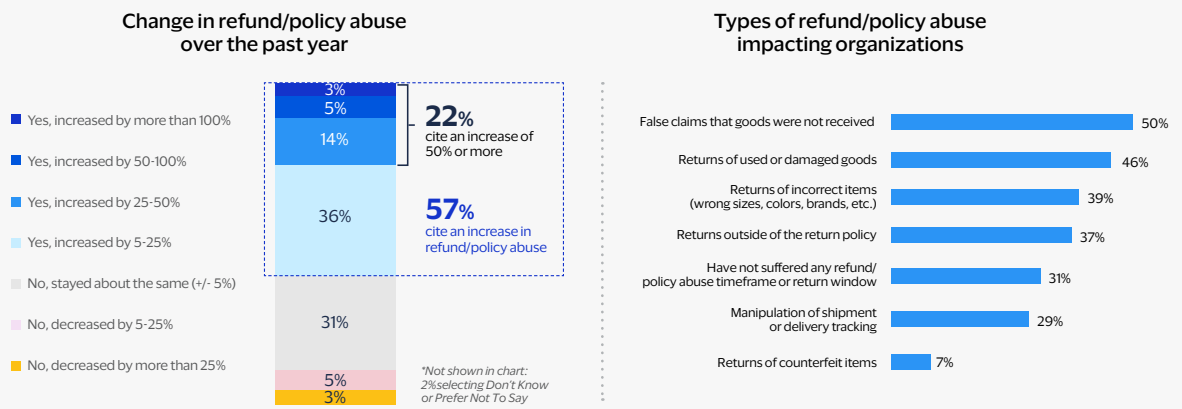


While it is encouraging to see merchants continuing to embrace compelling evidence as another approach for mitigating FPM, there remains potential opportunity to increase their win rate with these disputes, if they can collect and submit more of the relevant data points (where such data is available and relevant).

The final set of insights in this section shifts the focus from FPM to refund/policy abuse. This is a new topic covered by the survey this year, so these results will serve as a baseline for understanding the current state of refund/policy abuse and for tracking changes in this form of fraud over the years to come. Overall, most merchants report an increase in refund/policy abuse over the past year, with 57% indicating some increase, and 22% citing an increase of 50% or more (see Figure 33). While not quite as high as comparable figures for FPM, these data points reinforce the fact that refund/policy abuse is a significant — and growing — form of fraud.

Figure 33

Trends and types of refund/policy abuse (2025, fraud professionals)



Also shown in Figure 33 are the various types of refund/policy abuse, along with the shares of merchants each type has impacted over the past 12 months. The most common manifestations of refund/policy abuse are false claims that goods were not received, impacting half of all merchants, and returns of used or damaged goods, impacting 46%. Returns of incorrect items and items outside of the return window are fairly common, too, as is manipulation of shipment or delivery tracking information, each impacting between 30% and 40% of merchants globally. Returns of counterfeit items are the least common form of abuse, impacting just under 3 in 10. Notably, only 7% of merchants surveyed said they faced no refund/policy abuse in the past year, indicating that this form of fraud is essentially a universal threat that all merchants have cause to consider.

But like FPM, refund/policy abuse is a bigger issue for some merchants than others. Merchants in Asia, for instance, are significantly more likely to cite increases in refund/policy abuse versus those in North and Latin America. The same goes for enterprise merchants compared with SMBs. And non-MRC enterprises are more likely than MRC members to report increasing rates of refund/policy abuse, although it is worth noting that a large share of MRC members in this year's survey declined to answer this question.

Figure 34

Change in refund/policy abuse over the past year by region, size, and mrc membership (2025, fraud professionals)

Change in refund/policy abuse over the past year	2025	Region				Merchant size			Membership	
	Overall	North America	Europe	Asia-Pacific	Latin America	SMB	Mid-market	Enterprise	MRC sample	Non-MRC enterprises
Base	1,082	447	219	255	153	284	285	495	70	443
Net % citing any increase	**57%**	**55%**	**57%**	**68%**	**52%**	**48%**	**61%**	**62%**	**40%**	**63%**
Yes, increased by more than 100%	**3%**	3%	2%	3%	2%	4%	1%	3%	0%	3%
Yes, increased by 50-100%	**5%**	5%	4%	5%	4%	4%	5%	6%	6%	5%
Yes, increased by 25-50%	**14%**	11%	9%	22%	16%	12%	15%	15%	9%	16%
Yes, increased by 5-25%	**36%**	35%	42%	35%	30%	29%	40%	38%	26%	39%
No, stayed about the same (+/- 5%)	**31%**	33%	33%	23%	34%	40%	28%	27%	30%	27%
No, decreased by more than 25%	**8%**	8%	5%	11%	14%	8%	9%	9%	7%	9%
Don't know / we do not track OR Prefer not to say	3%	5%	5%	1%	0%	3%	2%	2%	24%	1%

= Significantly higher versus other segments = Significantly lower versus other segments

Overall, the themes and findings in this section paint a somewhat positive picture of merchants getting a better handle on the issue of FPM, in part by increasing the effectiveness of their anti-FPM strategies and in part by making greater use of compelling evidence to challenge and win the fraudulent FPM disputes that occur. But while progress is being made to thwart FPM, most merchants are now seeing an increase in refund/policy abuse. No doubt, the merchant community will be challenged to devise new strategies and adapt current tools and tactics to counter this rising threat, in 2025 and beyond.

5. Fraud management

This section of the report examines what merchants are doing, at both a strategic level and a tactical level, to manage and mitigate eCommerce fraud. Insights covered here include the strategic priorities that guide merchants' fraud management efforts, as well as the major challenges merchants face in devising and implementing their fraud management strategies.

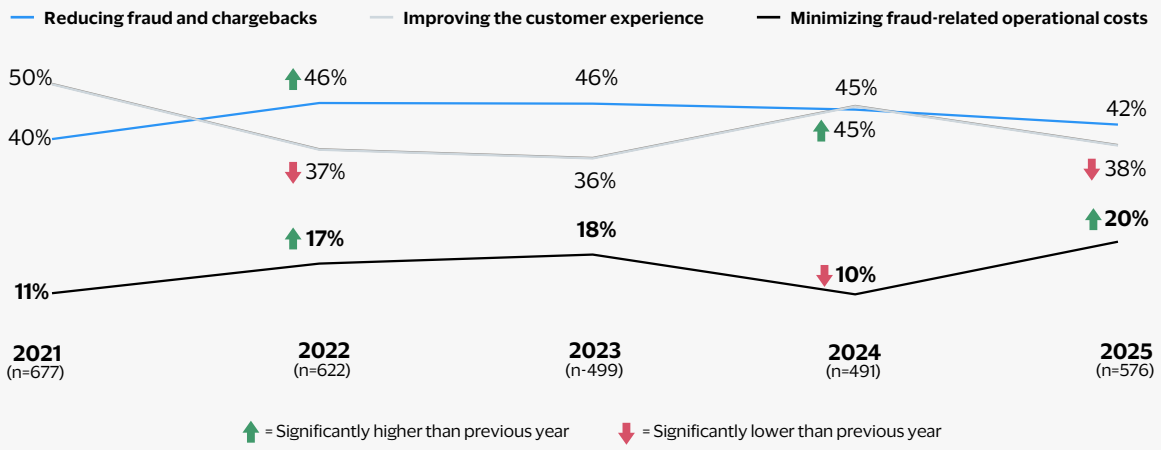
At the tactical level, this section also includes data showing how merchants approach manual-versus-digital fraud screening, how and where merchants monitor for fraud throughout the customer journey, and how merchants adopt and apply various fraud prevention tools and techniques, including those powered powered by AI and machine learning.

Reducing fraud and chargebacks still the top priority, but reducing costs rises in importance, while improving CX declines

Figure 35 shows how merchants have ranked their top fraud management priority in each of our surveys over the past five years.

Figure 35

Top fraud management priority (2021-2025, fraud professionals)

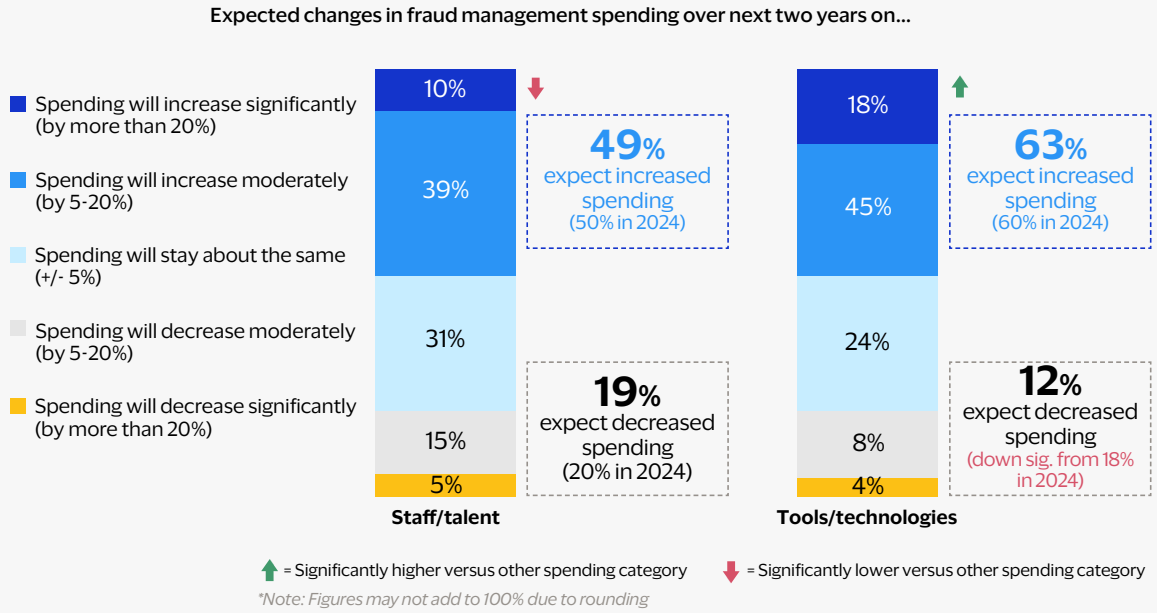


Since 2022, reducing fraud and chargebacks has been the priority selected by the largest share of merchants, and this year was no different in that regard: Over 4 in 10 fraud professionals say this remains their number one goal heading into 2025. What has changed this year is a significant decline in the share prioritizing improving the customer experience, in addition to a significant increase in the share of merchants focusing primarily on minimizing operational costs. This shift represents a reversal of the change in these two priorities that was captured in last year's report, when significantly more merchants prioritized improving CX rather than cost reduction. In fact, looking at the full five years of data shown in the chart, there seems to be a cyclical, see-saw relationship between these two priorities: A large share of merchants will deprioritize cost reduction relative to CX improvement for one year, then a similar share will shift focus back to cost reduction one to two years after.

What all of this means for merchant fraud professionals and fraud prevention solution providers over the next year is that we are now entering the phase of the cycle where many merchants are looking to "do more with less" by continuing to reduce fraud and chargebacks while also reducing the operational costs incurred by their fraud management efforts. Indeed, there is some support for this hypothesis in the results of a separate survey question asking senior fraud professionals what their expectations are for fraud management spending at their organization over the next two years (see Figure 36).

Figure 36

Expected change in fraud management spending over next two years



**Note: Figures may not add to 100% due to rounding*

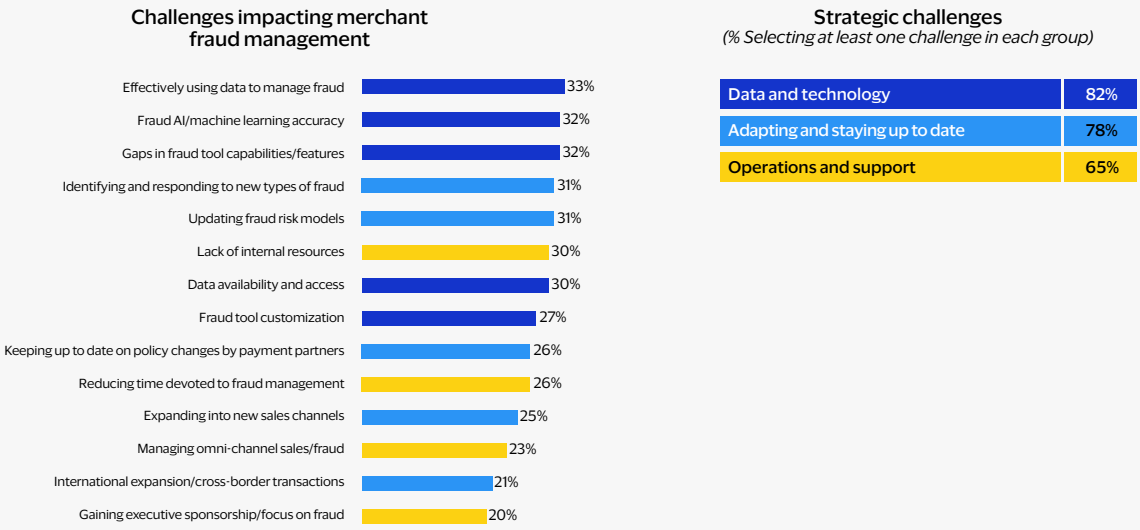
The majority (51%) expect spending on fraud management staff/talent to remain flat or decrease in the near future. Only 1 in 10 expects spending in this area to increase significantly. By contrast, 63% foresee increased investment in fraud management tools and technologies during this period, with nearly 2 in 10 expecting their organization to ramp up spending here by over 20%. In other words, merchants may be looking to manage and minimize costs, in part, by shifting more of their anti-fraud spending from human talent to tools and technologies. This strategic shift among merchant fraud professionals from spending and relying more on humans to spending and relying more on technology is a major and recurring theme in this year's survey results, reflecting an important trend taking place in the global marketplace.

Data and technology issues represent the biggest challenge for fraud pros, followed by difficulties staying up-to-date

As merchants increasingly rely on data and technology to manage fraud, it makes sense that they are increasingly focused on solving data and tech-related challenges. In fact, the top three challenges fraud professionals highlight in this year's survey all fit that description. These include effectively using data to manage fraud, ensuring the accuracy of AI/ML-based fraud tools, and overcoming gaps in fraud tool features and functionalities, and these issues each impact roughly one-third of merchants, globally (see Figure 37). Altogether, 67% claim one or more of these three challenges is negatively impacting their ability to manage fraud.

Figure 37

Fraud management challenges (2025, fraud professionals)

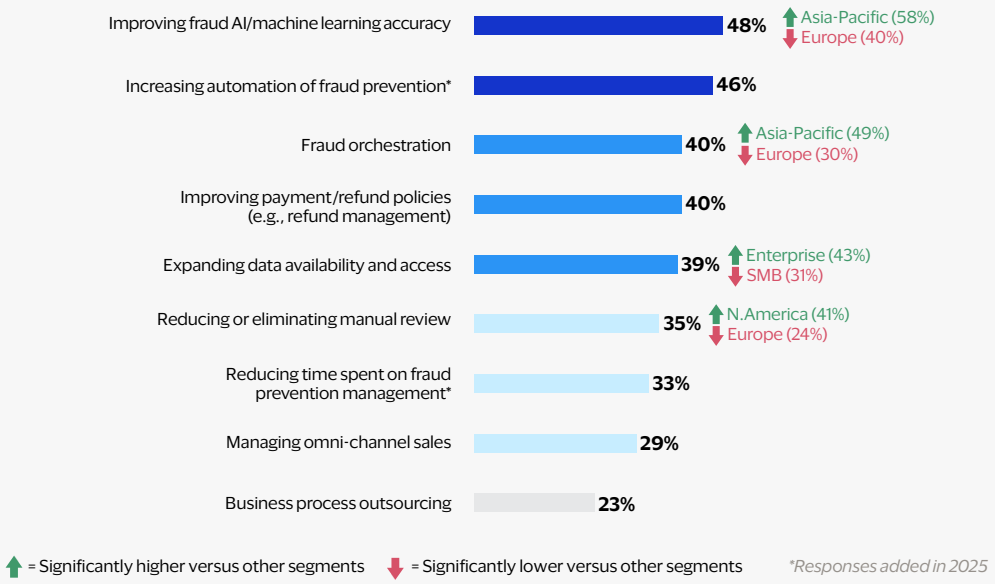


Another major difficulty merchants face is staying up-to-date, both in terms of understanding and countering new forms of fraud and in terms of updating their fraud risk models, so they remain as accurate and effective as possible amidst a constantly and dynamically evolving threat environment. And a third key obstacle hampering fraud management efforts is a lack of internal resources coupled with a lack of data availability and access, each hindering around 3 in 10 merchants globally.

Given the strategic imperatives they are prioritizing, as well as the major challenges they face, where are merchants most intent on making improvements to their fraud management programs? Figure 38 offers a glimpse of merchants' focus areas for 2025.

Figure 38

Top improvement areas for fraud management over the next 12 months



Once again, data and technology come to the fore, as improving AI/ML fraud tool accuracy, increasing automation, and expanding data availability and access all rank among the top five improvement areas, each a priority for 40% to 50% of merchants globally. Improving fraud orchestration and optimizing payment/refund policies are also top focus areas, both of which make sense given that gaps in fraud capabilities remains a top challenge and refund/policy abuse is emerging as a growing threat.

There are some differences in priorities across merchant segments: Those in Asia are significantly more likely to focus on AI/ML accuracy and fraud orchestration compared with those in Europe. Enterprise merchants are more apt to focus on expanding data availability and access versus SMBs. Finally, North American merchants are more likely than those in Europe to try to reduce or eliminate manual order review this year, with 41% of the former selecting this as a key focus area versus 24% of the latter.

While North American merchants may be especially eager to cut down on manual order review, they are reflective of a broader trend emerging in our recent years of survey data, which shows a general, global shift of merchants moving away from manual screening and toward digital screening instead. As illustrated by the data in Figure 39, merchants now screen over twice as many orders digitally as they do manually (52% versus 23%, respectively), and this gap has widened slightly, compared to where it was last year (51% digital versus 25% manual). In fact, merchants in APAC and small businesses significantly increased the share of orders they screen digitally over the past year, from 38% to 50% and from 40% to 50%. MRC members, in particular, are leading this shift to digital screening, as they now screen nearly 9 out of 10 orders (86%) digitally and only 3% manually. Non-MRC enterprises, by contrast, are lagging behind this trend, screening just 44% of orders digitally and 26% manually.

Figure 39

Digital versus manual order screening by region, size and MRC membership (2024-2025, fraud professionals)

Digital and manual fraud screening (Raw averages shown)	**2025**	**By region**				**By size**			**MRC members**	
		North America	Europe	Asia-Pacific	Latin America	SMB	Mid-market	Enterprise	MRC sample	Non-MRC enterprises
Base	524	245	77	139	57	127	144	242	52	203
Average % of orders screened digitally (via software or other technologies)	52%	54% (56%)	53% (54%)	50% (38%)	41% (48%)	50% (40%)	52% (48%)	51% (59%)	(87%)	44% (48%)
Average % of orders screened manually (via human analysis or judgment)	23%	25% (27%)	21% (18%)	24% (27%)	21% (21%)	27% (30%)	24% (26%)	22% (21%)	3% (4%)	26% (28%)
Average % of manually screened orders that are subsequently declined	19%	20%	16%	19%	16%	16%	19%	20%	23%	20%

= Significantly higher versus other segments = Significantly higher versus other segments (xx% = 2024 figures) (Significantly higher versus 2024) (Significantly lower versus 2024)

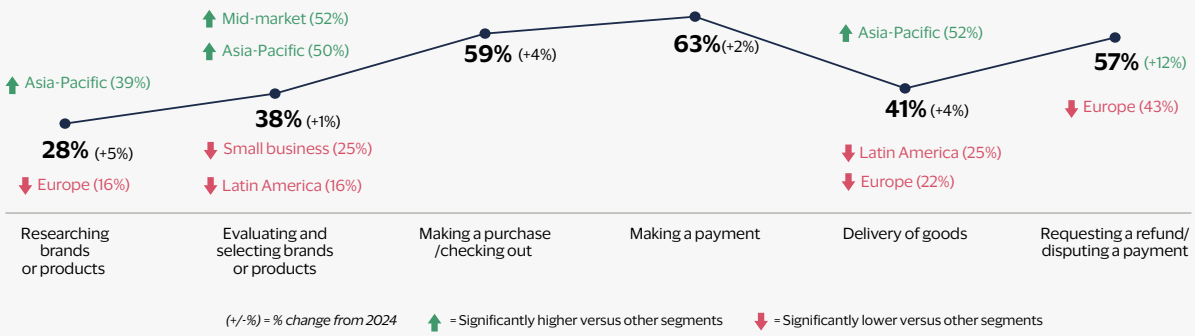
Also shown in Figure 39, is the share of manually screened orders that are subsequently declined, which averages right around one in five (19%) globally. This share of "manually declined" orders is remarkably consistent across merchants in all regions and size segments, as well as for MRC members and non-MRC enterprises. So while the level of manual screening may vary from merchant to merchant, the rate at which those manual reviews lead to declined orders is generally similar across the board.

Increasing application of fraud tools to monitor customer journey

Merchants' growing reliance on tools and technologies to manage fraud is further illustrated by the increase in the share of merchants applying tools to detect potential fraud signals at each stage of the typical customer journey. As the data in Figure 40 depicts, the share of merchants using fraud tools at each stage increased over the past year, and the share applying fraud tools at the final stage, when customers request a refund or dispute a payment, rose significantly from 45% to 57%.

Figure 40

Fraud monitoring throughout the customer journey (2024-2025, fraud professionals)



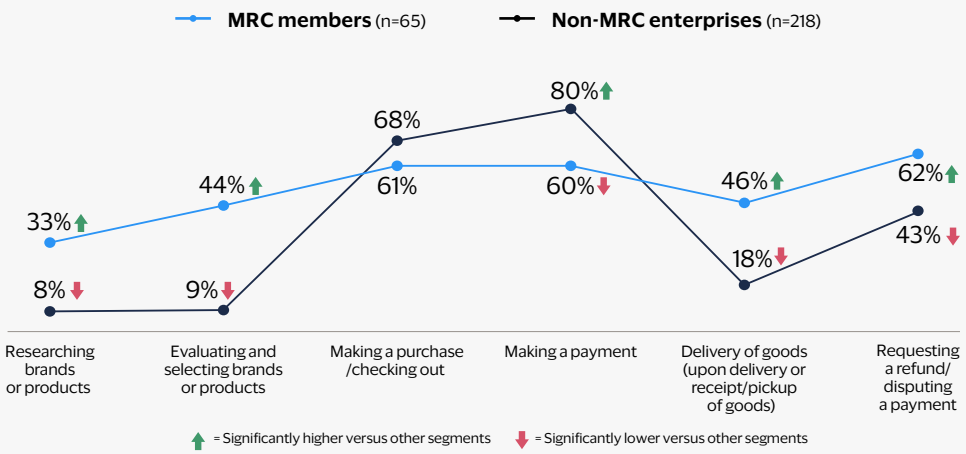
Globally, over half of merchants now monitor for fraud at the purchase/checkout and payment stages, as well as at the refund/dispute stage. But only a minority monitor for fraud at the pre-purchase stages and at the point of delivery or order fulfillment. This may be one of the outstanding "gaps in fraud tool functionalities" many merchants cite as a key challenge at the strategic level (see Figure 37).

There are also notable differences in fraud monitoring by geography, with merchants in Asia being significantly more likely to monitor at pre-purchase and delivery stages, while merchants in Europe and Latin America are less likely. European merchants also under-index on checking for fraud when customers request refunds or dispute payments; only 43% do so currently.

Another group that under-indexes at 43%, when it comes to monitoring for fraud at the refund/dispute stage, is MRC members (see Figure 41). This contrasts starkly with the 62% of non-MRC enterprises that apply tools to monitor for fraud at this stage. Similar discrepancies between these two groups are evident at the pre-purchase stages, as well, with non-MRC enterprises generally four to five times more likely to be monitoring at those stages. The pattern is reversed when it comes to monitoring fraud at purchase/checkout and at the point of payment. At these two stages, MRC members over-index, and this is especially the case for payment, where 80% of members scan for fraud, versus just 60% of non-member enterprises.

Figure 41

Fraud monitoring throughout the customer journey by MRC membership (2025, fraud professionals)

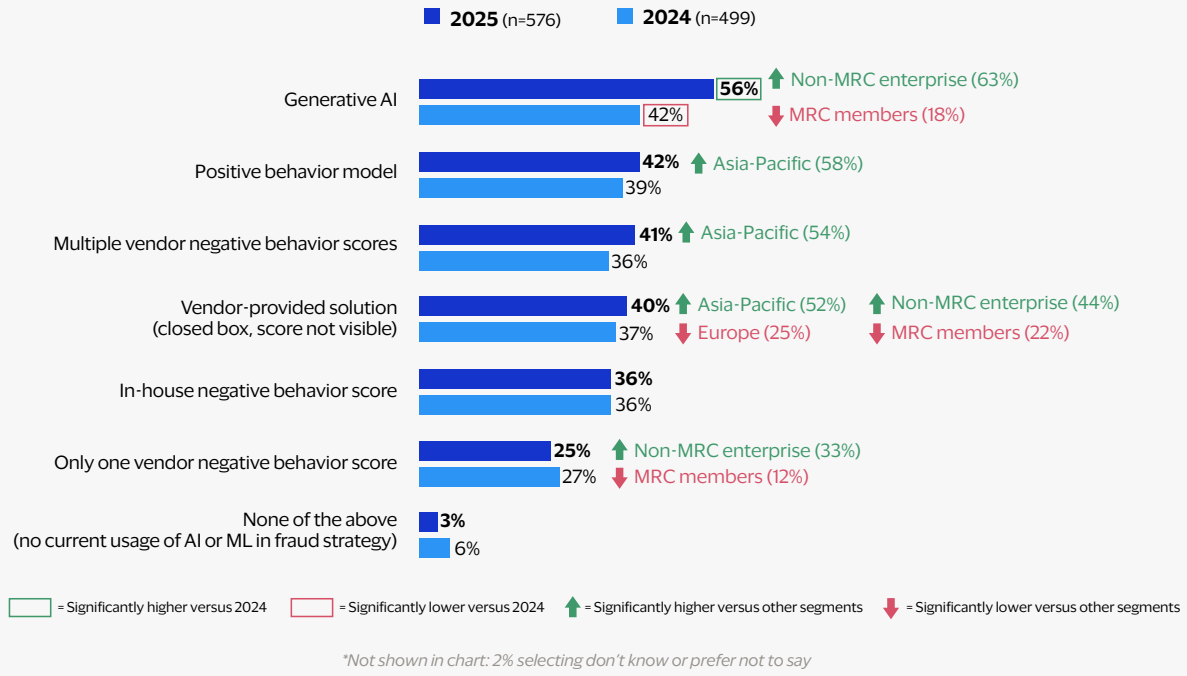


Merchants report continued, steady uptake of AI/ML-driven fraud tools

Our final set of insights shows how merchants continue to steadily adopt AI/ML-based fraud tools. The chart in Figure 42 compares the current usage rates of a range of these tools last year and this year, and the overall trend is clear to see: There are increases virtually across the board in the share of merchants using each tool. In the case of generative AI tools, in particular, the usage rate has spiked significantly year-over-year from 42% to 56%. In fact, only 3% of merchants in this year's survey claim they are not currently using any AI or ML fraud tools at all, signaling that there are very few in the market that have not yet invested in at least some tools or techniques powered by these advanced technologies.

Figure 42

Current usage of AI/ML-driven fraud management tools (2024-2025, fraud professionals)



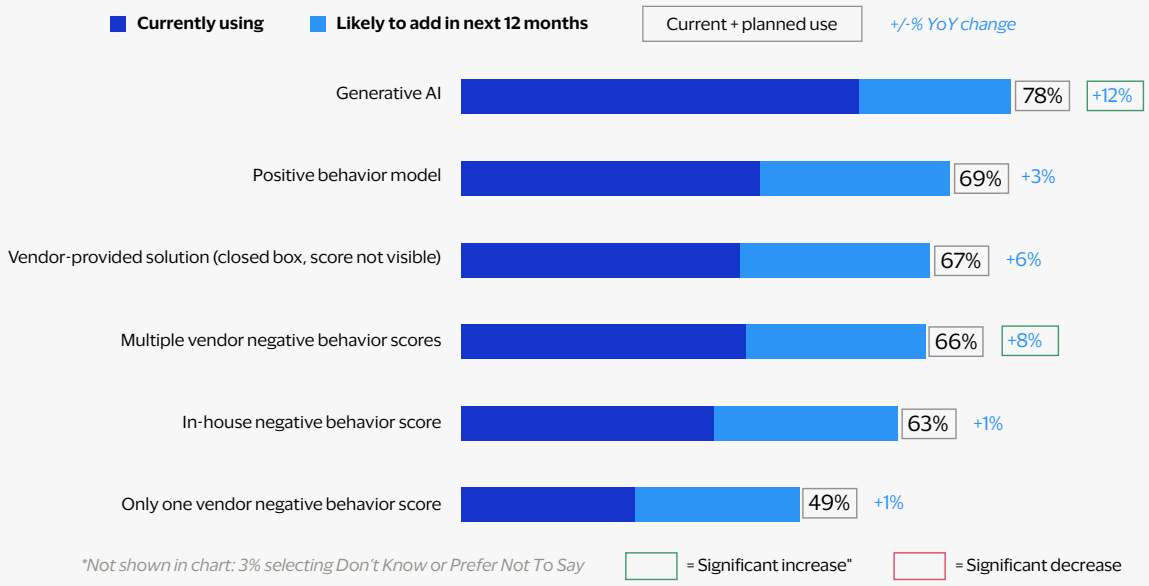
**Not shown in chart: 2% selecting don't know or prefer not to say*

As in other areas of data and tech adoption, merchants in Asia are leading the charge toward AI. Those in this region over-index significantly on current usage of positive behavior models, multiple-vendor negative behavior scores, and vendor-provided solutions (the latter of which is used by significantly fewer merchants in Europe). In addition, there is a striking difference in the usage rates of multiple AI/ML tools between MRC members and non-MRC enterprises, with the latter over-indexing significantly relative to the former on usage of generative AI, vendor-provided solutions, and single-vendor negative behavior scores.

Survey data also show that adoption of these kinds of tools and techniques is likely to continue apace throughout 2025 and beyond. Figure 43 displays the current proportion of merchants using each tool, as well as the share that say they are likely to consider adding in the next 12 months. By summing the current and planned usage percentages, we get a sense of the potential headroom for growth in the usage of each AI/ML tool over the next year. So, by the end of 2025, as many as 8 in 10 merchants (78%) may be using generative AI tools and usage rates for the rest may be hovering in the 60% to 70% range.

Figure 43

Current + planned usage of AI/ML-driven fraud management tools (2025, fraud professionals)



Overall, the data in this section clearly indicate an increasing lean into data and tech-based fraud management solutions among merchants worldwide. To the extent merchants can successfully implement and integrate these solutions, overcoming the major disconnects and obstacles that often hamper such efforts, this strategy of leaning into data and technology may serve them well in accomplishing all their strategic priorities of minimizing costs, improving CX and, most of all, reducing fraud and chargebacks.

Conclusion

The insights and trends discussed in this report highlight how complex and challenging it is for merchants to effectively manage both eCommerce payments and fraud in today's commercial environment.

Payment acceptance offerings and strategies continue to evolve as merchants strive to keep customers satisfied with new, convenient options like real-time payments, while at the same time minimizing the risks and costs. Third-party partners such as marketplaces, acquirers and gateways continue to be indispensable partners and enablers for merchant payment acceptance, helping them maximize sales and revenue while ensuring operations and integrations run smoothly and safely.

Merchants continue to track a broad range of key payment metrics and utilize a wide array of tools, techniques, and tactics to optimize payment management. 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 offerings and operations, they must also strive to improve their strategies and tactics for preventing and mitigating fraud. While there are encouraging signs this year that payment fraud is on the decline, merchants must be vigilant in defending against new and growing threats such as real-time payment fraud. This is especially the case as more merchants look to reduce costs in their fraud management operations, as cutting back on investment and talent in this area may yield short-term benefits at the cost of long-term harms and vulnerabilities.

Facing considerable challenges and obstacles in the realm of fraud management, many merchants are betting on data and technology to deliver solutions and outcomes that are both more effective and more cost-efficient than those they have relied on in the past. In particular, merchants seem intent on investing in AI- and ML-driven tools and platforms, meaning that cooperation between fraud professionals and IT/technology professionals may be increasingly critical for ensuring merchants remain protected from fraud over the coming months and years. Leveraging advanced technology to its maximum potential while tempering it well with human experience, knowledge, and judgment is the overarching goal for many fraud professionals today.

About the authors

Visa Acceptance Solutions

Visa Acceptance Solutions, a Visa division, is for businesses looking to build the payments experiences of the future. We utilize the strength of 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 30+ years of payments expertise, Visa Acceptance Solutions' leading-edge technologies, flexible infrastructure, and data-driven approach can help businesses thrive.

For more information, please visit: visaacceptance.com.

cybersource
A Visa Solution

Cybersource, part of the Visa Acceptance Solutions portfolio, provides a global payment management platform and fraud management system built on the Visa infrastructure. This solution enables businesses to reach their digital commerce goals by enhancing customer experiences and operating with agility, while helping grow revenues and mitigate risk.

For more information, please visit: cybersource.com

MRC

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.

VERIFI
A Visa Solution

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 losses, create operational efficiencies, and remove unnecessary fraud and first-party misuse disputes from the payment ecosystem.

For more information, please visit: verifi.com.

B2B International
a dentsu company

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.

Appendix: Survey questions asked

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 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?

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?

For more information please visit: visaacceptance.com.

VISA Acceptance Solutions