2024 Global eCommerce Payments & Fraud Report

25TH EDITION

MRC

VISA Acceptance Solutions

cybersource
A Visa Solution

VERIFI
A Visa Solution

Report Contents

Overview

The Merchant Risk Council (MRC), along with Visa Acceptance Solutions and Verifi, are proud to present the results of the 2024 Global eCommerce Payments & Fraud Survey. This is the 25th edition of this study, as Visa began researching and reporting on eCommerce fraud trends all the way back in 1999! As in years past, the primary purpose of this report is to convey transparent and unbiased research on global merchants' perceptions of current trends and topics related to eCommerce payments and fraud.

This year's report is based on a global survey of more than 1,100 MRC and non-MRC merchants. The survey sample includes a diverse mix of small businesses (SMBs), mid-market and enterprise merchants, representing organizations based in more than 35 countries throughout North America and Europe, as well as the Asia-Pacific (APAC) and Latin America (LATAM) regions.

Utilizing this survey data, the report delves into today's rapidly changing payments landscape to illuminate the range of different payment acceptance, management and partnership practices merchants are deploying, as well as the reasons they are adopting these payment strategies and tactics in the current environment. In addition, the report provides the MRC merchant community with 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.

The MRC extends its gratitude to all participating merchants for taking the time to complete the online survey, to Visa Acceptance Solutions and Verifi for managing the research, and to B2B International for directing the research program and analyzing the data.

Survey Firmographics

The survey for this year's report was fielded from October to December 2023. In total, 1,166 merchants involved in eCommerce fraud and payment management (including 147 MRC members) completed the survey. The survey sample includes merchants based in 37 countries, spanning four major geographic regions, with broad representation across revenue tiers, sales channels, and eCommerce categories. The breakdown of the survey sample by region, annual revenue and primary eCommerce category is detailed in the figures below.

Figure 1

Share Of Sample By Geographic Region

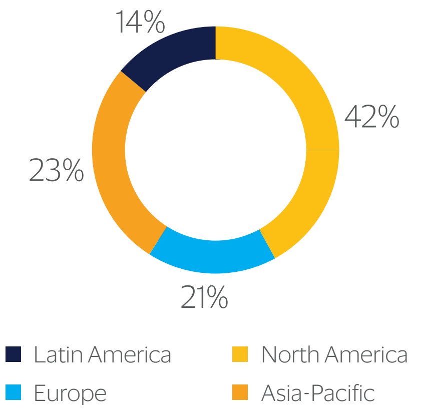


Figure 2

Share Of Sample By Merchant Size

(Annual eCommerce Revenue)

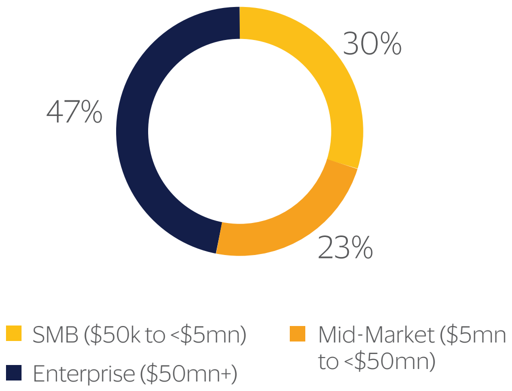
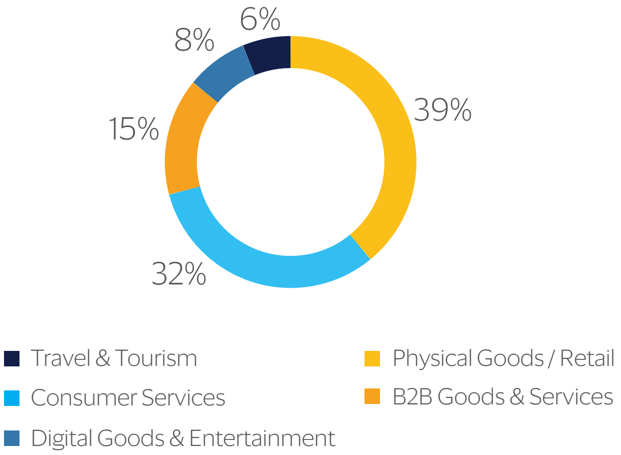


Figure 3

Share Of Survey Sample By Primary eCommerce Category



Among the 147 MRC members in this year's survey sample, six in 10 (60%) are based in North America, with the remainder based primarily in Europe (26%). Nine out of 10 participating MRC merchants are fraud and payments professionals at large enterprises, which generate more than $50 million in annual eCommerce revenue. Due to changes in this year's survey to improve the survey experience and data quality, various questions now have smaller base sizes than in prior years.

Executive Summary

The key insights from the 2024 Global eCommerce Payments & Fraud Survey are organized into six sections in this report. The first three sections examine the current state of eCommerce payments, while the last three sections address trends and topics related to eCommerce fraud. Altogether, the insights and findings reported in these sections convey a detailed and nuanced picture of the state of eCommerce payments and fraud today from the perspective of merchants around the world.

The key themes and findings in each section of the report are:

1. Payment Acceptance

Acceptance Offerings Continue To Evolve, With Real-Time Payments And Buy Now, Pay Later On The Rise

- Merchants typically accept four to five different payment methods. Globally, roughly three-quarters of eCommerce merchants accept cards and digital wallet payments, and most also take debit transfers and mobile payments.

- Eight in 10 (82%) merchants began accepting at least one new payment method over the past year. Real-time payments (RTP) and buy now, pay later (BNPL) are among the fastest-growing acceptance methods, along with digital wallets, debit transfers, and mobile payments.

But As Acceptance Grows, So Does Fraud Risk: The Most Popular Payment Methods Are Thought To Have The Highest Fraud Rates

- Card and digital wallet payments, followed by mobile payments and debit transfers are perceived as having the highest fraud rates, even though they are the most widely accepted.

Merchants See Real-Time Payments As An Overall Plus

- Merchants overwhelmingly agree that real-time payments will complement credit card payments, contributing positively to the financial ecosystem.

2. Payment Tactics & Metrics

Merchants Make Use Of Multiple Tactics To Ensure Secure, Reliable, Customer-Friendly Payment Experiences

- Nine out of 10 merchants encourage customers to pay via certain, preferred payment methods, usually by prioritizing or promoting these methods at checkout. Primary motivations for merchants doing this are to decrease fraud risks and minimize processing costs.

- More than 90% of merchants employ at least one tool or technique designed to boost payment authorization rates, for instance, automated retries or intelligent payment routing. Merchants are increasingly making use of third-party data to improve the effectiveness of authorization-boosting tactics.

- Payment tokenization is another important tactic showing steady uptake among global merchants, with around two-thirds now using some form of tokenization to strengthen payment security and maximize authorizations.

As Payment Methods And Tactics Proliferate, Merchants Feel Pressure To Track A Multitude Of Metrics

- Merchants consider a wide range of payment-related metrics highly important as key performance indicators (KPIs) for their business. Out of 13 metrics tested in this year’s survey, every one was rated “very” or “extremely important” by more than half of merchants surveyed.

3. Payment Partnerships

Third-Party Marketplaces Help Merchants Maximize Reach And Minimize Costs To Serve Customers At Scale

- Eight in 10 merchants globally, sell goods or services through third-party marketplaces, like Amazon, eBay, and Alibaba. Gaining access to large numbers of loyal customers and providing a good customer experience are the primary reasons so many merchants use marketplaces.

- Usage of third-party marketplaces varies significantly across merchants in different regions and size segments. For instance, Mercado Libre was the most widely used marketplace among Latin American merchants in this year’s survey, whereas Amazon was most popular in every other region. Nearly nine out of 10 midsize merchants sell on at least one third-party marketplace, versus only roughly 75% of small and enterprise merchants.

Processors And Acquirers Remain Critical Partners For Enabling Merchant Payments Across Markets & Methods

- On average, merchants use four different payment gateways or processors and three different acquiring banks to support eCommerce payments. Key motivations for using multiple acquirer partners include overall flexibility in payment processing, as well as improving authorization rates and maximizing geographic coverage.

4. Fraud Opportunities

Fraud On The Rise, With First-Party Misuse A Growing Problem

- Merchants are facing a wider range of different types of fraud attacks, as the number of different attacks experienced by the average merchant rose significantly and several types of fraud increased significantly in incidence, compared with last year. The types of fraud that merchants are seeing more of this year include first-party misuse, account takeover, loyalty fraud, and triangulation schemes.

- Refund/discount abuse and first-party misuse now top the list as the most common forms of fraud, each impacting nearly half of merchants, globally. Phishing, card testing, and identity theft remain prevalent threats, as well.

- Fraud is particularly problematic for merchants in North America and for MRC members, as these merchants report a significantly larger volume and variety of fraud attacks.

Merchants Struggle With Resourcing And Operational Challenges, Inhibiting Their Efforts To Effectively Manage Fraud

- Lack of internal resources dedicated to fraud management represents the biggest challenge overall faced by merchant fraud professionals. Other key challenges impacting more than half of merchants globally include staying up to date on new attacks, risk models, and rule changes; managing fraud across different sales channels and geographic markets; and leveraging data and tools to effectively prevent and mitigate fraud.

- Lack of internal resources, gaps in fraud tool functionalities, and responding to new types of attacks rank among the top five challenges faced by merchants in every region and sector.

Fraud Creates Both Financial And Customer Experience Impacts, Eroding Brand Reputation

- Merchants report considerable direct losses from eCommerce fraud, in terms of lost revenues and fraudulently obtained goods and services. For instance, merchants estimate that 3% of their total eCommerce revenue is lost to fraud each year, and a similar share of total eCommerce orders turn out to be fraudulent.

- Fraud also puts a strain on merchant relationships with customers and with key commercial partners, like card issuers and fulfillment vendors. For instance, merchants reject an estimated 6% of eCommerce orders received annually due to fraud suspicions, and most report “customer insult” (or false positive) rates between 2% and 10%. Merchants also report low win rates—below 20%—on fraud-coded chargebacks and disputes.

5. First-Party Misuse

First-Party Misuse Is On The Rise, Especially Among Enterprise And North American Merchants

- More than six in 10 merchants cite an increase in first-party misuse (FPM) over the past year, continuing last year's trend of rising incidence. Increasing eCommerce sales and rising inflation are seen as the fundamental drivers of this trend, although several merchants also cite increasing customer awareness of this form of fraud, exacerbated by a proliferation of online "tools and tips," for how to successfully perpetrate it.

- First-party misuse also accounts for an increasing share of all fraudulent disputes, according to merchants. They believe attempts to obtain free goods and transaction descriptor confusion are primarily driving this trend.

- North American merchants are significantly more likely than merchants in other regions to report an increase in first-party misuse. Enterprises are also more likely than SMBs and mid-market merchants to cite rising incidence.

With A Growing Need To Combat First-Party Misuse, Merchants Are Pulling Multiple Levers To Find A Solution

- Merchants are utilizing multiple strategies and techniques in their efforts to effectively counter the rising threat of first-party misuse. Various tools and tactics related to flagging & checking, verification & identification, and enhanced requirements are considered the most effective, compared with customer notifications and filing & fighting.

- Compelling evidence rules and processes set forth by card brands are widely known and widely used among merchants globally. Eight in 10 report submitting compelling evidence to resolve FPM disputes, and a similar majority are aware of the major updates that card networks made to their compelling evidence policies in recent years.

- Over three-quarters (77%) of merchants have utilized card networks' updated compelling evidence rules to successfully block or reverse first-party misuse disputes. In general, merchants see the recent rule updates as helpful, especially those that have successfully applied them.

6. Fraud Management

Merchants Taking Divergent Paths On Fraud Strategy & Spending

- Each year, the survey asks merchants which of three goals they are prioritizing in their fraud management strategy: minimizing operational costs, improving the customer experience, or reducing fraud and chargebacks. Heading into 2024, significantly fewer merchants are prioritizing cost minimization as the top imperative driving their fraud management strategies. But merchants are now equally split on prioritizing improving the customer experience and reducing fraud and chargebacks.

- Similarly, around half of merchants plan to increase spending on fraud management tools / technologies and staff/talent over the next two years, but the other half are intent on either doing more with their current spending levels or on finding ways to reduce investment while maintaining or improving performance. Spending plans differ significantly by region and size segment, indicating merchants playing in similar markets may be taking similar approaches, even as their strategies diverge from those in other geographies and revenue tiers.

- Merchants show more consensus when it comes to which aspects of fraud management they will focus on improving over the next year, with the majority citing AI/ML-driven fraud management tools, fraud orchestration, and refund management as top priorities.

Merchants Are Also Acting Differently At The Tactical Level, Although Nearly All Intend To Adopt AI-Driven Tools & Techniques

- When it comes to the tactics and tools merchants use to prevent and mitigate payment fraud, more than half are using technologies to monitor and signal potential fraud at the purchase and payment stages of the customer journey. But most do not monitor for fraud at pre- or post-purchase stages, including refund requests or disputes. This may be one of the “gaps in fraud tool functionalities” many merchants cite as a key strategic challenge.

- When it comes to manual versus digital (or automated) order screening for fraud, merchants estimate they apply roughly a 2-to-1 ratio, screening approximately 25% of orders manually, and 50% of orders digitally. But this balance between manual and digital order screening differs significantly across merchants in separate regions and size segments.

- It’s clear that AI- and ML-driven fraud tools are of great interest to merchants. On average, merchants say they are currently using one to two AI/ML-based fraud tools or techniques. While less than half say they are currently using any one particular AI/ML-based fraud tool tested in the survey, usage of these tools and techniques is likely to grow rapidly this year, as the majority say they expect to start using each tool and technique tested in the survey in the near future.

1. Payment Acceptance

In the first three sections of this report, the focus is on eCommerce payments. Specifically, these sections delve into how merchants are being paid by customers, which payment tactics and metrics are integral to their business, and what kinds of third-party payment partners and enablers they rely on to support payment experiences and operations.

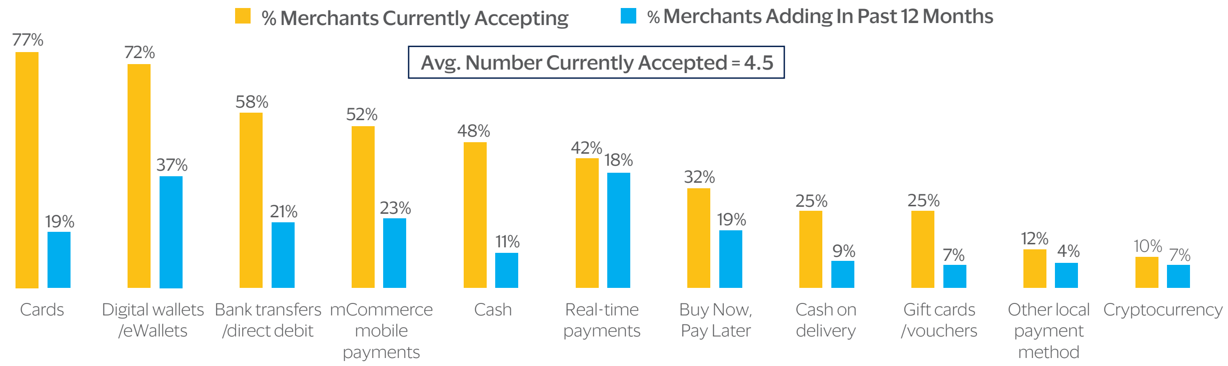
This section starts by examining how merchants are accepting payments from customers, i.e., which payment methods they are accepting, what their views and approaches are when it comes to adopting new payment methods like real-time payments, and which payment methods they associate with higher risks of fraud.

Acceptance Offerings Continue To Evolve, With Real-Time Payments And Buy Now, Pay Later On The Rise

Consistent with prior years of our study, merchants continue to accept four to five different payment methods on average from their customers. Card and digital wallet payments are the top two acceptance methods, each used by roughly three-quarters of eCommerce merchants worldwide. Most merchants accept debit transfers and mobile payments as well (see Figure 4).

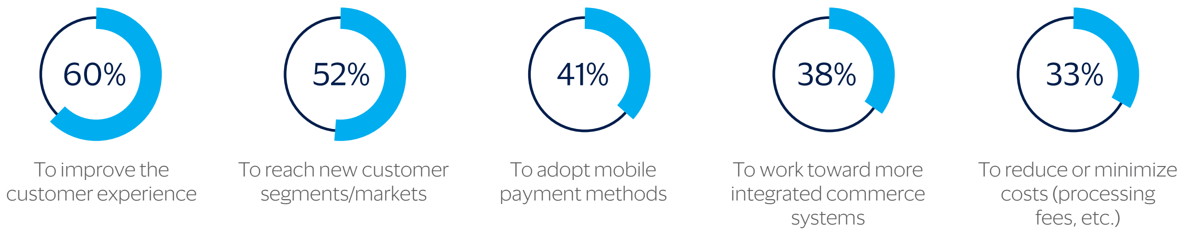
While those top acceptance methods are widely used by merchants in all regions, some methods are used much more in certain markets than others: for instance, cash on delivery is accepted by more than one-third of merchants in APAC, versus less than 25% of merchants in other regions. And gift cards and vouchers are far more popular among North American merchants than those operating elsewhere.

Figure 4: Payment Methods Currently Accepted / Added In Past Year & Top Reasons For Adding New Methods



*Not shown in chart: 11% indicating no new payment methods added in the past year

Top 5 Reasons For Adding New Payment Methods



As consumer expectations and preferences regarding digital payments evolve, so too, must merchant acceptance offerings. Among the fastest-growing new payment methods are digital wallets (currently accepted by 72%), mobile payments (52%), real-time payments (42%) and buy now, pay later (32%). The survey shows that a large share of merchants now accepting these types of payments added them within the past year. Adding new methods is especially important for merchants looking to improve the customer experience and/or reach new customers. In fact, these are the top two motivations merchants cite in the survey for adopting new acceptance offerings (see Figure 4).

It is important to highlight that MRC members take a distinct approach to payment acceptance compared with non-MRC enterprises within our survey sample. 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 alternative methods like real-time payments, cash on delivery, and cryptocurrency. MRC members also over-index on using gift cards/vouchers and alternative/local digital payment methods such as Boleto and Pix (see Figure 5).

Figure 5: Payment Methods Currently Accepted - MRC Members Vs. Non-MRC Enterprises

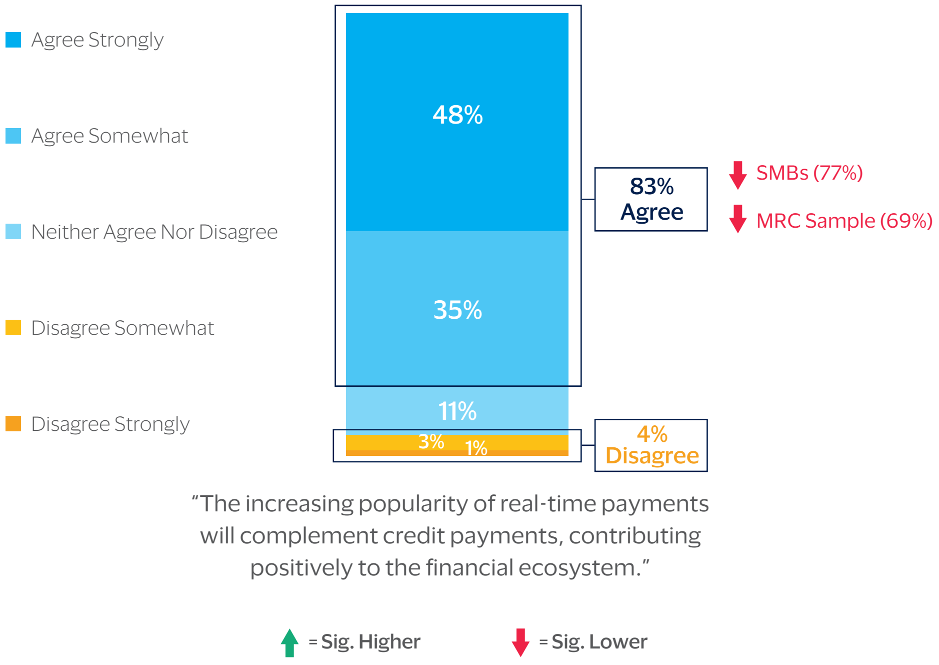
% Merchants Currently Accepting Each Method	**Overall**	**By MRC Membership**	
		MRC Members	Non-MRC Enterprises
Base	*667*	*67*	*228*
Cards	**77%**	100%	73%
Digital wallets/eWallets	**72%**	84%	72%
Bank Tranfers/direct debit	**58%**	61%	58%
mCommerce mobile payments	**52%**	39%	58%
Cash	**48%**	39%	46%
Real-time payments	**42%**	22%	46%
Buy Now, Pay Later	**32%**	36%	33%
Cash on delivery	**25%**	6%	28%
Gift cards/vouchers	**25%**	43%	28%
Other local payment methods (Boleto, Neosurf, Pix,POL, etc)	**12%**	37%	11%
Cryptocurrency	**10%**	3%	15%
AVG # ACCEPTED	*4.5*	*4.7*	*4.7*

🟩 = Sig. Higher 🟥 = Sig. Lower

Merchants View Real-Time Payments As An Overall Plus

Given the rapid rise of real-time payments, a new question was added to the survey this year to understand merchant sentiment surrounding this new way for consumers to pay. Overall, merchants overwhelmingly agree that the rise of real-time payments represents a positive development for the financial ecosystem, since real-time payments can complement credit card payments. As shown in Figure 6, 83% of merchants agree with this sort of statement and only 4% disagree.

Figure 6: Merchant Views On Real-Time Payments

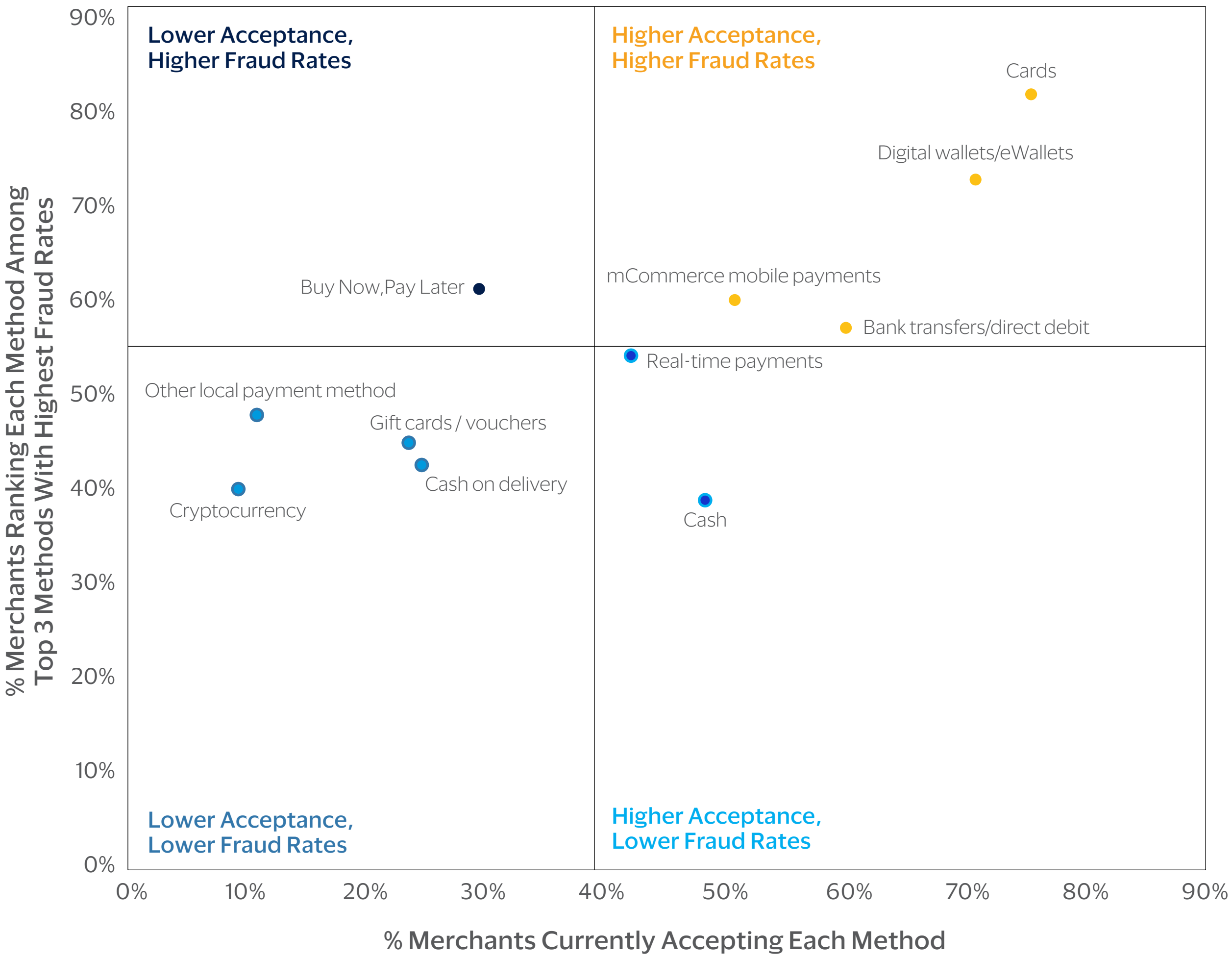


Not all merchants are so optimistic about the emergence of real-time payments, though; for instance, only 77% of SMBs and 69% of MRC members indicated agreement with the previous statement. But overall, merchants clearly view this new payment method in a positive light. No doubt, both merchants and their partners in the credit card industry will be keeping a close eye on the continued emergence and impact of real-time payments in the years to come.

As Acceptance Grows, So Does Fraud Risk: Merchants Associate The Most Widely Accepted Payment Methods With the Highest Risk

Among the new insights emerging from this year's survey is a strong and direct link, in merchants' eyes, between how widely accepted and used a certain payment method is and how high the risk or rate of fraud is for that method. When asked which of their accepted payment methods had the highest rates of fraud, merchants cited cards and digital wallets as the top two, followed by mobile payments, BNPL, debit transfers, and real-time payments. This ranking basically mirrors the ranking of the most widely accepted payment methods (shown in Figure 4), suggesting that as merchants and customers increasingly embrace a given payment method, so too, do fraudsters looking to maliciously profit from it.

Figure 7: Payment Method Acceptance Versus Fraud Rates



The strong correlation between payment method acceptance and fraud rates is illustrated in Figure 7. Payment and fraud professionals should take note of this dynamic and consider its implications when thinking about future plans and strategies related to payment acceptance and fraud management.

2. Payment Tactics & Metrics

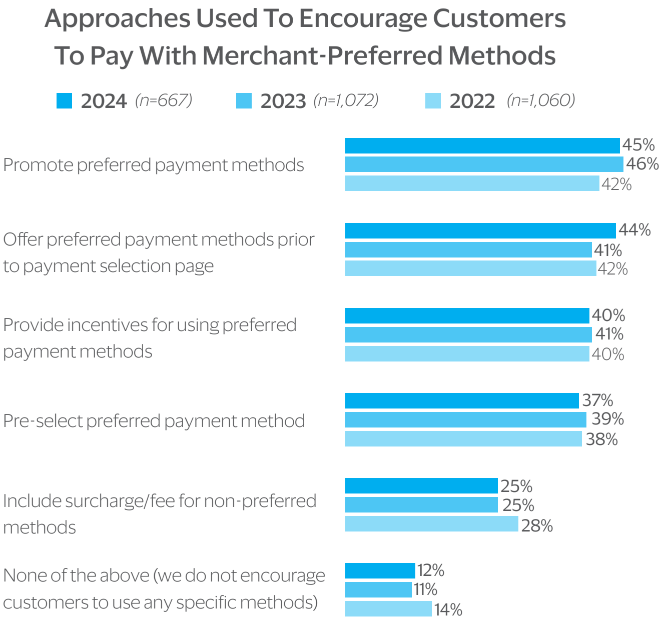
This section drills down on merchants' acceptance strategies to reveal which payment tactics and metrics they consider integral to their business. Specific topics covered here include whether and how merchants encourage customers to use certain payment methods, what kinds of tools and techniques merchants use to increase authorization rates, and how and why merchants employ payment tokenization. This section also examines which payment-related metrics merchants view as highly important for gauging the health and success of their business.

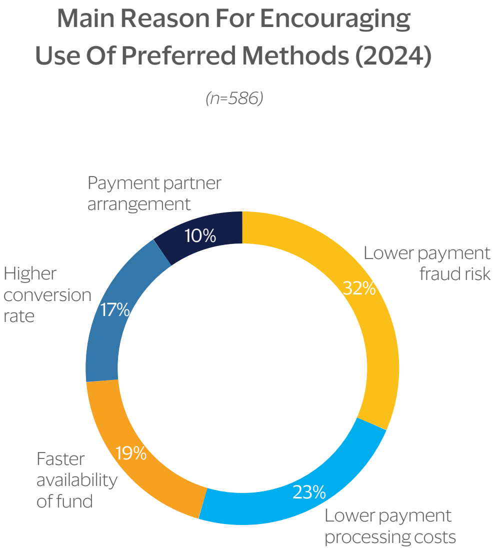
Merchants Employ Multiple Key Tactics To Provide Customers With Smooth, Secure, And Satisfactory Payment Experiences

While merchants are typically willing to accept several different payment methods, the vast majority (88%) take proactive steps to encourage customers to pay via certain preferred methods (see Figure 8).

Top tactics for encouraging the use of preferred methods include promoting these methods through messaging or incentives offered to customers as well as prioritizing or pre-selecting these methods when customers start the checkout process. Some merchants (25%) even go as far as to include extra fees or surcharges for customers who opt to pay with other non-preferred methods. The main reasons merchants encourage customers to pay with certain methods are to lower fraud risk and to minimize processing costs, although some cite faster availability of funds and higher conversion rates as other key benefits.

Figure 8: Encouraging Customers To Use Preferred Payment Methods (2022-2024)

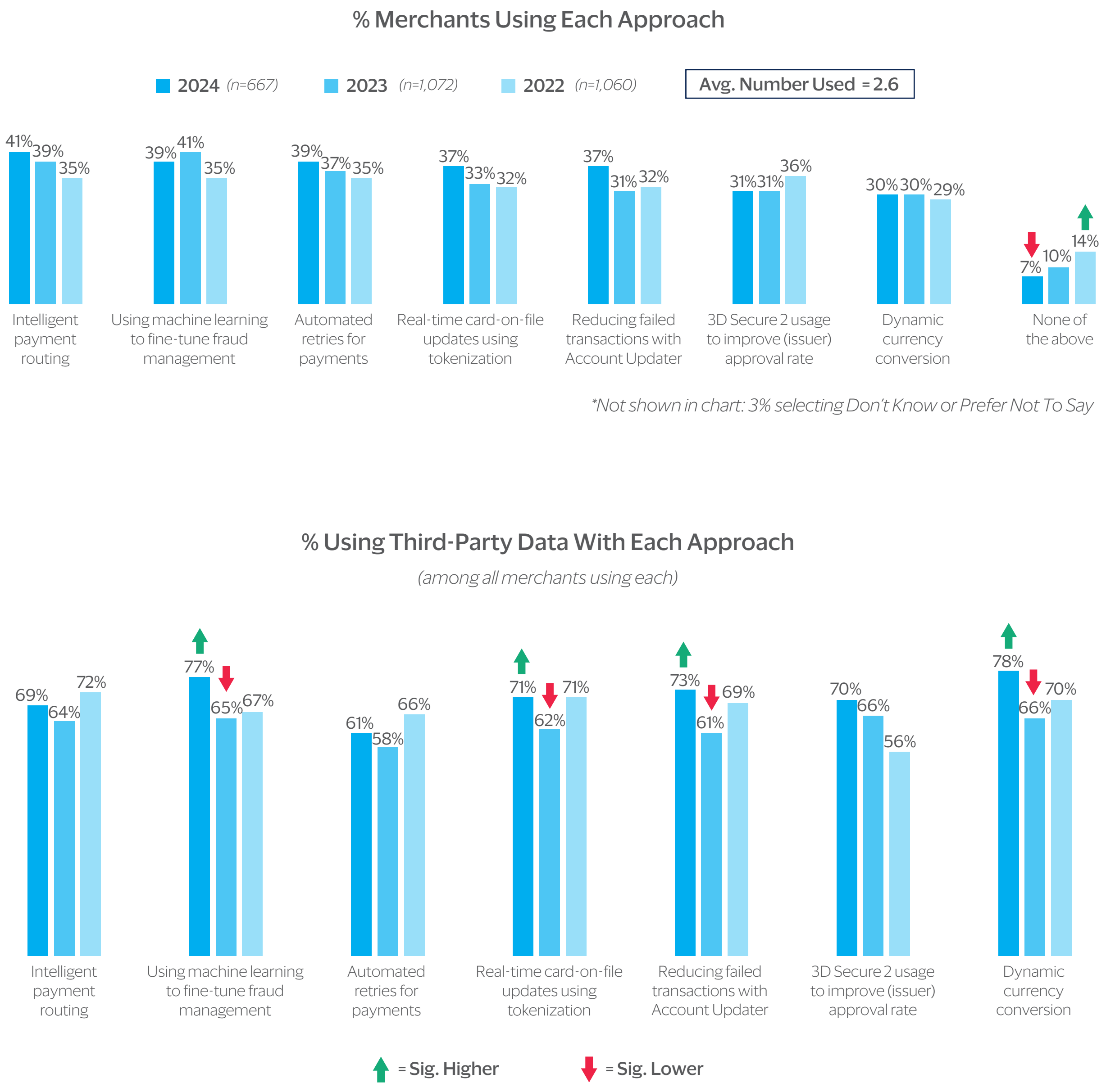




Despite the range of benefits cited by merchants above, MRC members are far less likely to nudge customers toward using specific payment methods: While 91% of non-MRC enterprises encourage payments via preferred methods, only around half (57%) of MRC merchants do so.

A second tactical area covered by the survey involves tools and techniques used by merchants to maximize payment authorization rates. Over the past three years of the survey, merchants have increasingly adopted a range of different authorization-related tools and techniques, with 93% in this year's survey using at least one of those shown in Figure 9 and the average merchant employing two to three.

Figure 9: Usage Of Authorization-Related Tools And Techniques (2022-2024)



**Not shown in chart: 3% selecting Don't Know or Prefer Not To Say*

Widely used authorization-boosting tactics include intelligent payment routing, use of machine learning to fine-tune fraud management, and automated retries for payments that do not go through initially. Usage of both real-time card-on-file updates and account updater solutions to reduce failed transactions has also increased among merchants over the past year.

As shown in Figure 10, enterprise merchants are significantly more likely and SMBs are significantly less likely to use many authorization-related tactics, in particular, intelligent payment routing, card-on-file updates, and 3D Secure 2. Also, MRC members are more apt than non-MRC enterprises to use automated retries, account updater tools, and 3D Secure 2.

Figure 10: Usage Of Authorization-Related Tools & Techniques – By Merchant Size & MRC Membership

% Using Each Approach	**Overall**	**By Size**			**By MRC Membership**	
		SMB	Mid-Market	Enterprise	MRC Members	Non-MRC Enterprises
Intelligent payment routing	**41%**	34%	42%	47%	52%	45%
Using machine learning to fine-tune fraud management	**39%**	33%	39%	43%	39%	44%
Automated retries for payments	**39%**	31%	41%	43%	66%	37%
Real-time card-on-file updates using tokenization	**37%**	32%	30%	44%	46%	43%
Reducing failed transactions with Account Updater	**37%**	34%	37%	38%	60%	32%
3D Secure 2 usage to improve (issuer) approval rate	**31%**	21%	28%	40%	58%	35%
Dynamic currency conversion	**30%**	26%	32%	32%	21%	35%
None of the above (no methods added)	**7%**	13%	4%	4%	3%	4%

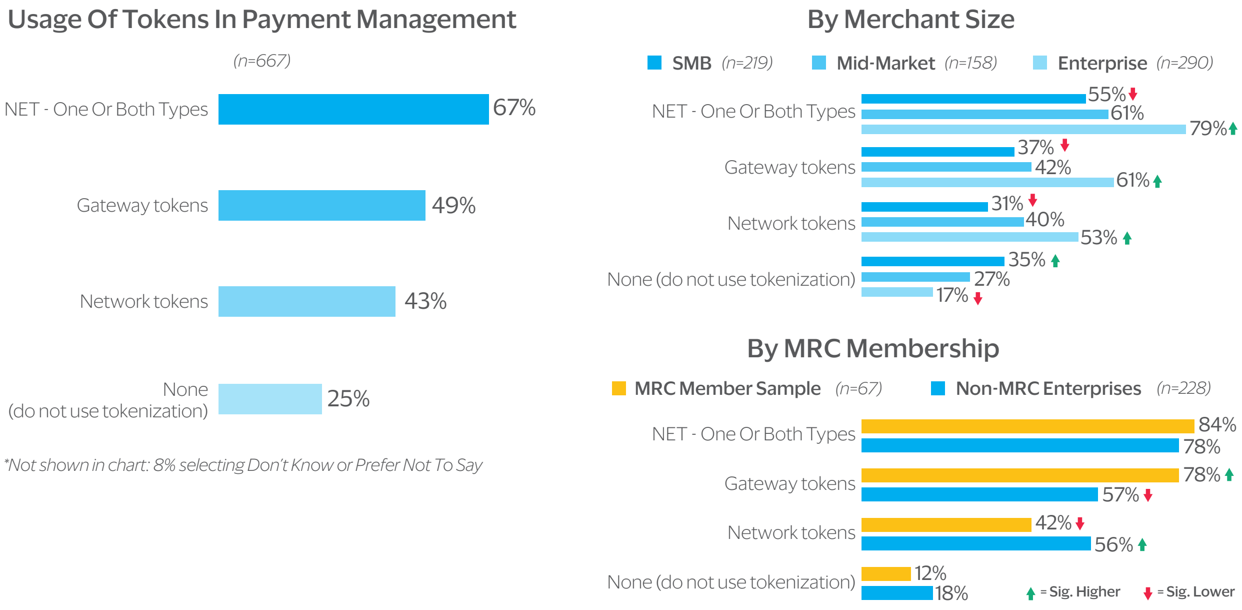
🟩 = Sig. Higher vs. Other Segments 🟥 = Sig. Lower vs. Other Segments

The last tactical topic addressed in the payments section of this year's survey is usage of tokenization in payment management. In this context, we define tokenization as replacing sensitive customer information with a unique identifier; using gateway tokens sponsored by payment gateways, acquirers, et cetera; or using network tokens sponsored by major card networks.

Whereas the vast majority of merchants employ tactics to promote preferred payment methods and boost authorization rates, many have not yet implemented tokenization. Globally, the survey shows two-thirds of merchants currently use some form of tokenization in payment management, but usage of both gateway and network tokens still hovers below 50% (see Figure 11).

As illustrated by the charts on the right-hand side of Figure 11, enterprise merchants are clearly driving adoption of tokenization, with 79% indicating that they use one or both types of tokens asked about in the survey. By contrast, only just over half (55%) of SMBs are using any form of tokenization currently.

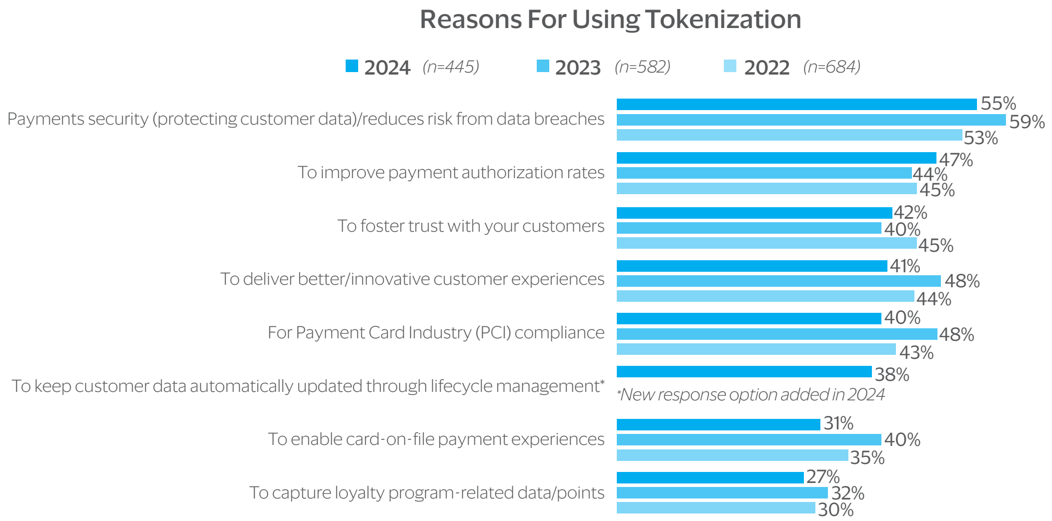
Figure 11: Usage Of Tokenization In Payment Management – Overall And By Merchant Size & MRC Membership



*Not shown in chart: 8% selecting Don't Know or Prefer Not To Say

It is also worth noting that MRC members show a much stronger preference for using gateway tokens than non-MRC enterprises. Nearly eight in 10 MRC merchants utilize gateway tokens, compared with only 57% of non-MRC enterprises. When it comes to network tokens, this pattern is reversed, as less than half of MRC members use network tokens, compared with 56% of non-MRC enterprises. This difference in usage may be driven by the distinct motivations these two groups have for using tokenization, which are examined later in this section (see Figure 13).

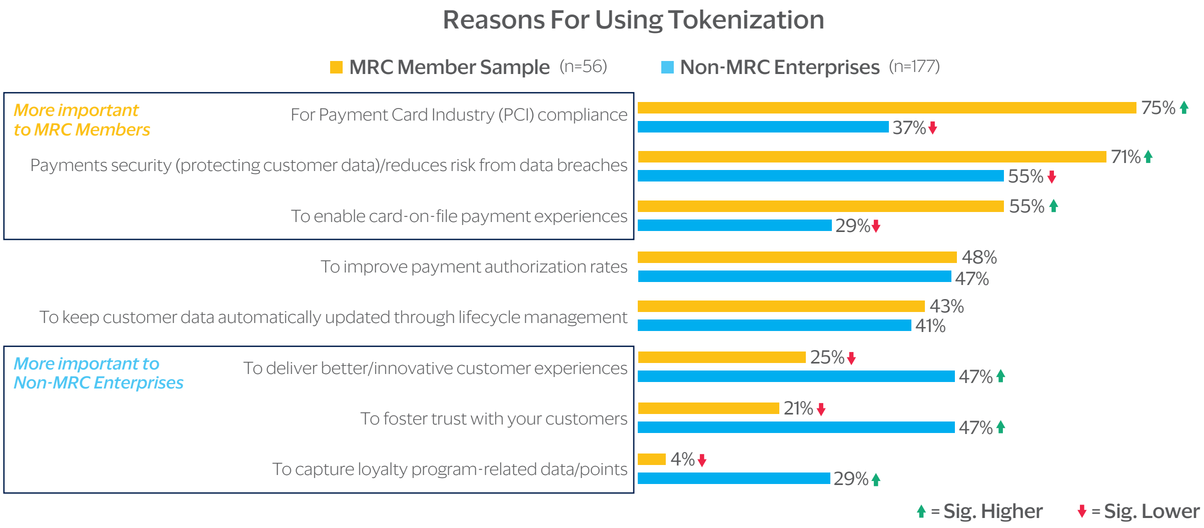
Figure 12: Reasons For Using Tokenization In Payment Management (2022-2024)



Why do merchants use tokenization in payment management? Primarily to improve data security and reduce the risk stemming from data breaches (the answer selected by the majority of merchants in the survey when asked this question, as shown in Figure 12). But improved authorization rates and the ability to foster greater trust with customers and provide them with better, more innovative payment experiences are also salient motivations cited by many merchants.

To understand why the usage of gateway versus network tokens differs significantly for MRC merchants and non-MRC enterprises, it may help to consider that they cite very distinct motivations for employing tokenization (see Figure 13). For MRC merchants, key motivations include PCI compliance, improved payments security, and enablement of card-on-file experiences. In contrast, non-MRC enterprises are much more likely to cite delivering better customer experiences, fostering trust with customers, and capturing loyalty program-related data as key reasons for employing tactics. Both merchants and providers of tokenization-related services should take these distinct rationales into account when partnering in this area.

Figure 13: Reasons For Using Tokenization In Payment Management – By MRC Membership

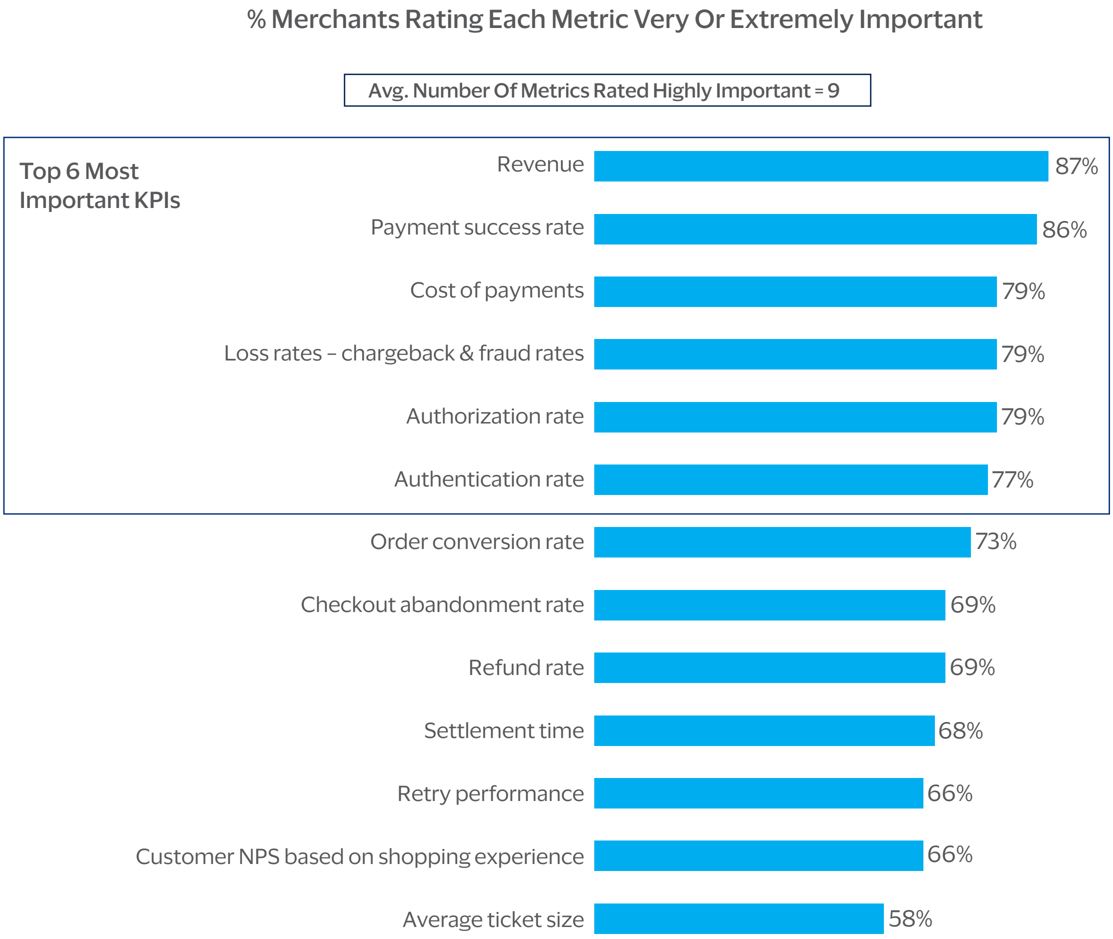


As Acceptance Methods And Payment Tactics Proliferate, Merchants See A Need To Track A Multitude Of Payment Metrics

As merchants accept more payment methods, face a wider range of fraud attacks, and implement many payment-related tactics and techniques, they may be feeling increased pressure to monitor and analyze a potentially dizzying array of payment-related metrics, or Key Performance Indicators (KPIs). When asked the importance of 13 different payment KPIs in this year's survey, more than half of merchants rated every single metric as "very" or "extremely" important to their business (see Figure 14).

The most critical metrics—each rated highly important by more than three-quarters of merchants globally—include revenue, success rate, cost of payments, loss rate, authorization rate, and authentication rate. The six KPIs listed above may form the 'core metrics' that merchant payment professionals are most intent on tracking, but the other seven are also considered highly important by the majority of payment professionals. These include abandonment rate, refund rate, settlement time, retry performance, customer NPS, and average ticket size.

Figure 14: Importance Of Payment Management KPIs



The overall theme in the data is that most merchants consider most or all of these payment metrics business-critical indicators. But digging deeper, the survey data indicates that certain merchant segments may be concerning themselves mainly with a subset of these metrics, while others may be trying to track the whole set.

Figure 15: Importance Of Payment Management KPIs – By Region & MRC Membership

% Merchants Rating Each Metric Very Or Extremely Important	**Overall**	**By Region**				**By MRC Membership**	
		North America	Europe	Asia Pacific	Latin America	MRC Sample	Non-MRC Enterprises
Base	*667*	*248*	*159*	*172*	*88*	*67*	*228*
Revenue	**87%**	90%	86%	80%	91%	93%	87%
Payment success rate	**86%**	87%	86%	85%	89%	96%	84%
Cost of payments	**79%**	79%	78%	78%	85%	72%	79%
Loss rates – chargeback & fraud rates	**79%**	77%	77%	77%	90%	76%	81%
Authorization rate	**79%**	81%	82%	69%	86%	93%	81%
Authentication rate	**77%**	82%	77%	69%	78%	78%	77%
Order conversion rate	**73%**	76%	70%	68%	82%	81%	76%
Checkout abandonment rate	**69%**	69%	70%	64%	76%	72%	73%
Refund rate	**69%**	73%	64%	66%	72%	34%	77%
Settlement time	**68%**	70%	62%	70%	70%	43%	71%
Retry performance	**66%**	66%	71%	60%	72%	61%	71%
Customer Net Promoter Score (NPS) based on shopping experience	**66%**	65%	65%	64%	75%	48%	73%
Average ticket size	**58%**	65%	57%	48%	59%	39%	65%
AVG # RATED HIGHLY IMPORTANT	*8.8*	***11.0***	***7.9***	***7.5***	***10.0***	***6.6***	***9.6***

🟩 = Sig. Higher vs. Other Segments 🟥 = Sig. Lower vs. Other Segments

Note in the bottom row of the table in Figure 15 the significant differences in the average number of KPIs rated highly important by merchants in Europe and APAC (each rating less than eight metrics highly important), versus those in North America and LATAM (each rating 10 or more highly important). Similarly, MRC members identify a much smaller range of KPIs as critically important than non-MRC enterprises. MRC members are mainly concerned with the top six metrics, while non-MRC enterprises are more likely to also monitor the 'long tail' of other KPIs.

Given the importance merchants place on all of these indicators, a comprehensive strategy and effective toolkit for collecting, monitoring, and utilizing this kind of payment data must be integral to any merchant's payment management strategy.

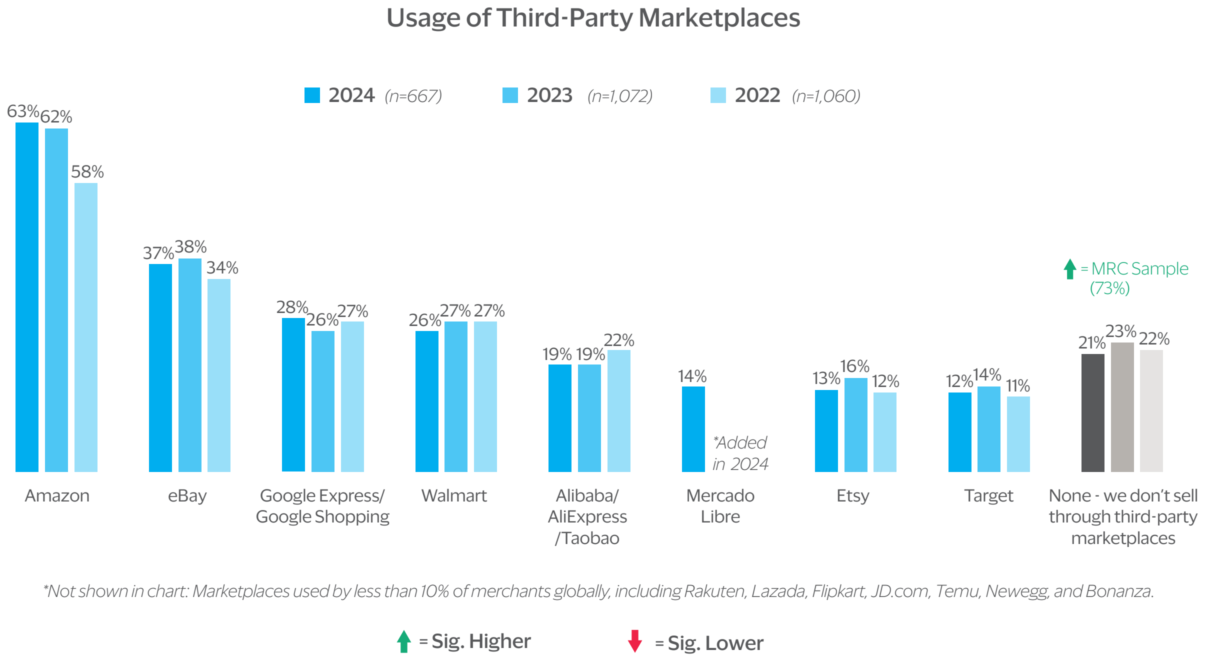
3. Payment Partnerships

In this final section centered around eCommerce payments, the focus is on how merchants team up with various third-party payment enablers to provide satisfying payment experiences to consumers and to ensure smooth, secure, and profitable processing of payment transactions.

Third-Party Marketplaces Help Merchants Maximize Reach And Minimize Costs While Serving Customers At Scale

In prior years, this study has shown that third-party marketplaces are instrumental partners for merchants looking to access large numbers of loyal customers and to provide them with good customer experiences beyond those offered at their own brand's storefronts. This basic theme was once again echoed by this year's survey, which shows around eight in 10 merchants are using at least one third-party marketplace to sell to customers (see Figure 16).

Figure 16: Usage Of Third-Party Marketplaces (2022-2024)



Not shown in chart: Marketplaces used by less than 10% of merchants globally, including Rakuten, Lazada, Flipkart, JD.com, Temu, Newegg, and Bonanza.

Amazon again tops the list of marketplace partners, with more than six in 10 globally selling through the eCommerce behemoth's shopping platform, nearly twice the usage rate of any other marketplace listed in the survey.
Other major marketplace partners include eBay, Google, Walmart, Alibaba, Mercado Libre, Etsy, and Target.

Drilling down, though, the data become far more varied, in terms of the marketplaces merchants partner with across different regions and size segments. As shown in Figure 17, key marketplace partners vary significantly by region, with eBay and Etsy more widely used by merchants in North America and Europe, Walmart more widely used in North and Latin America, and Alibaba, Rakuten, Lazada, Flipkart, and JD.com primarily used by merchants in APAC.

Figure 17: Usage Of Third-Party Marketplaces By Region, Merchant Size & MRC Membership

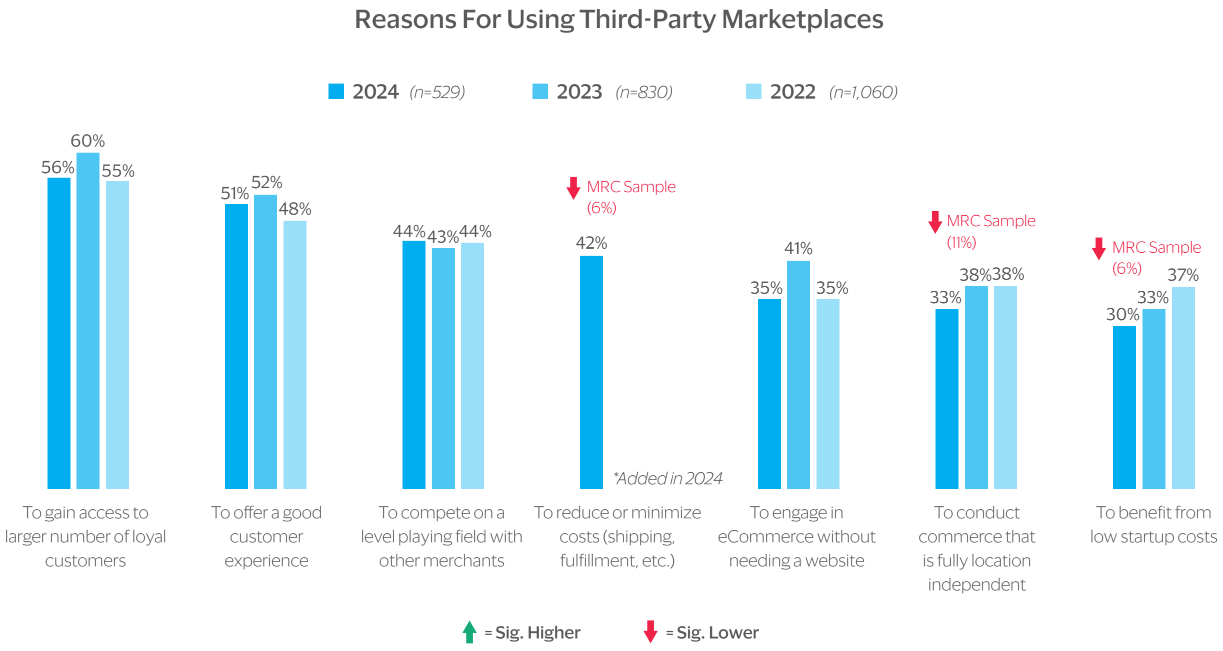
% Selling Through Each Third-Party Marketplace	**Overall**	**By Region**				**By Size**			**By MRC Membership**	
		North America	Europe	Asia Pacific	Latin America	SMB	Mid-Market	Enterprises	MRC Sample	Non-MRC Enterprises
Base	*667*	*248*	*159*	*172*	*88*	*219*	*158*	*290*	*67*	*228*
Amazon	63%	63%	62%	62%	70%	60%	72%	61%	18%	73%
eBay	37%	39%	45%	32%	24%	33%	40%	37%	9%	45%
Google Express/Google Shopping	28%	28%	27%	27%	34%	30%	28%	27%	3%	34%
Walmart	26%	38%	14%	19%	26%	23%	25%	29%	12%	33%
Alibaba/AliExpress/Taobao	19%	14%	11%	34%	22%	16%	22%	21%	3%	26%
Mercado Libre	14%	4%	6%	5%	74%	12%	13%	16%	1%	20%
Etsy	13%	19%	16%	5%	5%	11%	16%	12%	0%	15%
Target	12%	19%	7%	10%	6%	5%	15%	16%	6%	18%
Rakuten	9%	8%	6%	16%	2%	4%	12%	11%	0%	14%
Lazada	8%	1%	0%	28%	2%	7%	10%	8%	0%	10%
Flipkart	8%	6%	4%	15%	2%	5%	7%	10%	0%	13%
JD.com	5%	3%	2%	13%	2%	1%	8%	7%	1%	9%
Temu	5%	6%	4%	4%	5%	3%	4%	7%	0%	9%
Newegg	4%	6%	3%	2%	3%	4%	1%	5%	1%	6%
Bonanza	3%	2%	1%	5%	5%	2%	3%	3%	0%	4%
None of the Above (we do not sell through marketplaces)	21%	24%	25%	16%	13%	24%	13%	23%	73%	10%

🟩 = **Sig. Higher vs. Other Segments** 🟥 = **Sig. Lower vs. Other Segments**

There is also a notable difference in usage of marketplaces by size segment. This is indicated by the data in the bottom row of the table in Figure 17 showing that nearly nine in 10 mid-market merchants sell through at least one marketplace, versus roughly three-quarters of SMBs and enterprises. In particular, midsize merchants are significantly more likely to sell through Amazon. This data suggest Amazon may be of more value—or more importance—as a commercial partner for midsize merchants than for SMBs and large enterprises.

The other difference illustrated by the data in Figure 17 is that unlike merchants in every other segment covered by the survey, most MRC members do not consider third-party marketplaces to be critical partners for their business. Only around one-quarter of members use them, in contrast to nine out of 10 non-MRC enterprises.

Figure 18: Reasons For Using Third-Party Marketplaces



The stark difference in usage of marketplaces between MRC members and non-MRC enterprises is partly explained by additional data from the survey (shown in Figure 18). Here, it is clear that MRC merchants see less benefit or value in selling through marketplaces (such as reduced shipping costs and the ability to conduct location-independent commerce). For most, though, online marketplaces continue to be key partners that provide access to large numbers of loyal customers and satisfy those customers with good shopping and payment experiences.

Payment Gateways And Acquirers Remain Key Back-End Partners For Enabling Merchant Payments Across Methods And Markets

Shifting focus to payment partners that support merchant payments on the back end, this year's survey reinforces another running theme from prior years: that usage of multiple payment gateways or processors, as well as multiple acquiring banks, is a core aspect of merchants' payment management strategies.

Globally, the average merchant partners with four different payment gateways or processors and three to four acquiring banks (see Figure 19). But there are notable differences by region and size segment: North American merchants and SMBs use fewer of each type of partner compared with merchants based in other regions and those generating higher annual revenues. In addition, MRC members use significantly fewer gateway or processor partners than non-MRC enterprises.

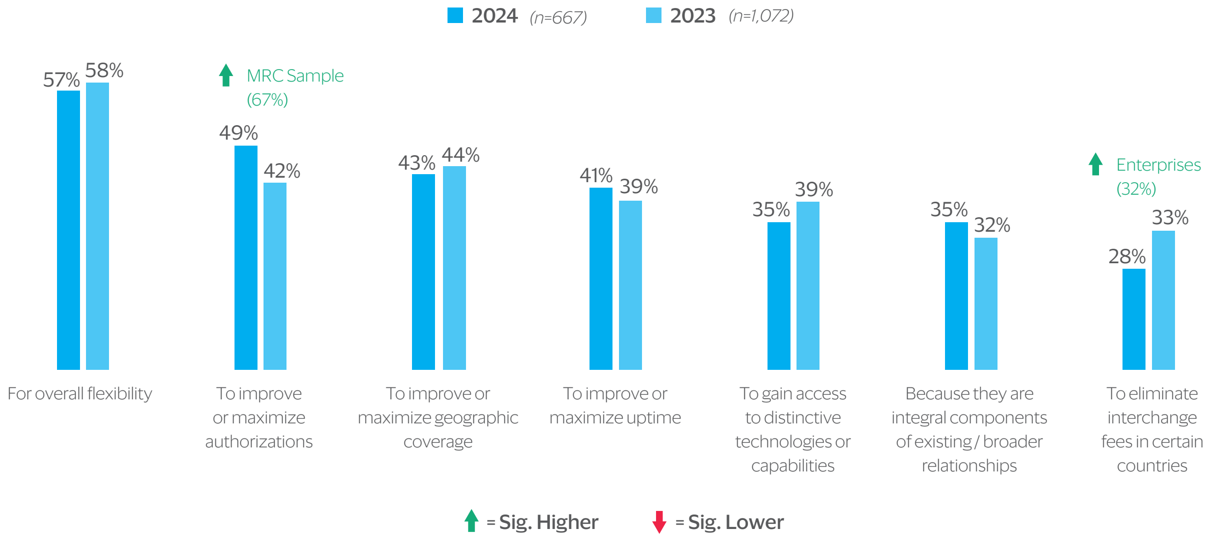
Figure 19: Usage Of Gateways & Acquirers And Reasons For Using Multiple Acquirers

Usage of Payment Processors and Acquiring Banks

Usage Of Payment Partners *(Trimmed averages shown)*	**Overall 2023**	**Overall 2024**	**By Region**				**By Size**			**By MRC Membership**	
			North America	Europe	Asia Pacific	Latin America	SMB	Mid-Market	Enterprises	MRC Sample	Non-MRC Enterprises
# Of Payment Gateway Or Processor Connections Currently Supported	3.9	**4.1**	3.7	4.2	4.4	4.3	3.5	4.4	4.3	3.5	4.5
# of Merchant Acquiring Banks Currently Used	3.4	**3.4**	3.0	3.6	3.7	3.9	2.9	3.6	3.7	3.3	3.8

🟩 = Sig. Higher 🟥 = Sig. Lower

Reasons For Using Multiple Acquiring Banks



These differences in numbers of acquirer partners are likely linked to the core rationales or benefits merchants highlight in the bar chart at the bottom of the figure. For merchants in North America, SMBs, and MRC members, the types of benefits displayed here—e.g., operational flexibility, improved authorization rates and uptimes, and increased geographic coverage—are presumably less salient and/or sufficiently obtainable through a smaller number of acquiring partners.

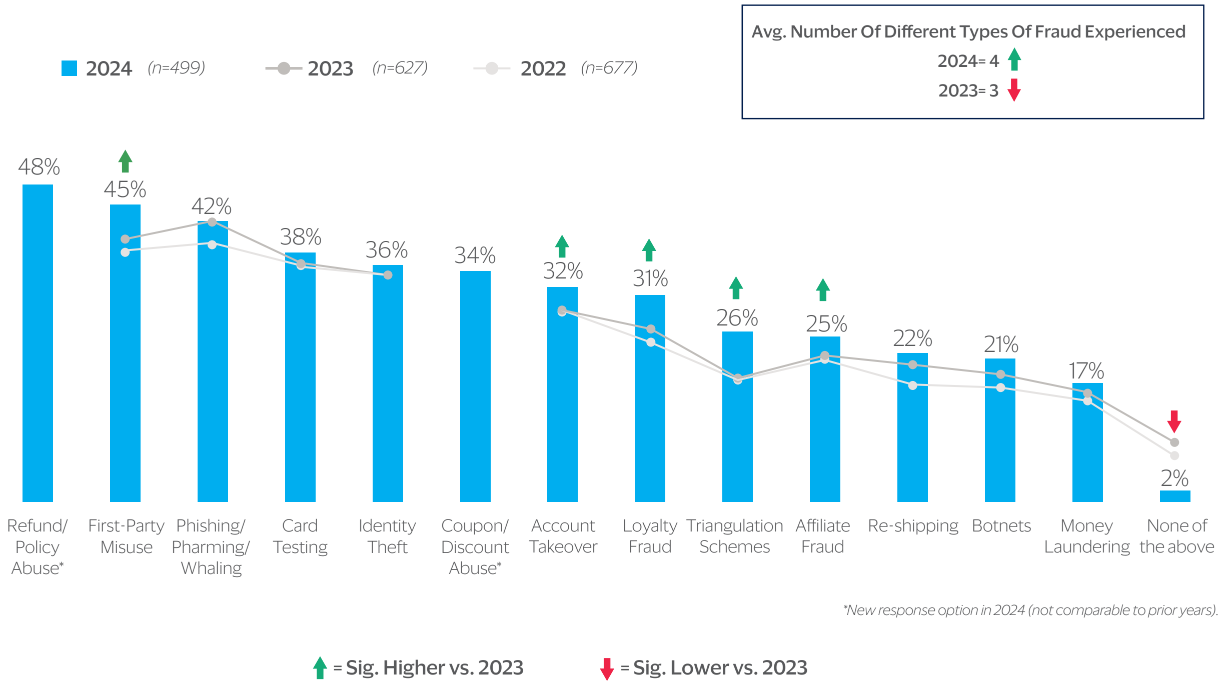
4. Fraud Opportunities

The remaining sections of this report focus on key topics and trends related to payment fraud in the eCommerce realm. This section examines insights regarding the top fraud challenges merchants have faced in the past 12 months, as well as the impacts of fraud on merchant businesses.

Fraud Rates Are Rising Overall, With First-Party Misuse A Particular Problem

Merchants are facing more fraud attacks than they have in prior years. The number of different types of fraud experienced by the average merchant this year rose from three to four (see Figure 20). In particular, merchants cite increased rates of first-party misuse, account takeover, loyalty fraud, triangulation schemes, and affiliate fraud than those reported in 2022 and 2023.

Figure 20: Types of Fraud Experienced By Merchants (2022-2024)



*New response option in 2024 (not comparable to prior years).

The top two types of fraud, each impacting just under half of merchants globally, are refund/policy abuse and first-party misuse. These fraud threats are especially difficult to counter because they are not related to attacks stopped in real time; rather, they generally occur post-purchase as customers and/or fraudsters attempt to obtain merchant goods or services for free. Thwarting these forms of fraud requires merchants to apply multiple tools and tactics pre- and post-purchase.

Figure 21: Top Fraud Attacks Experienced In Past 12 Months - By Region & Size Segment

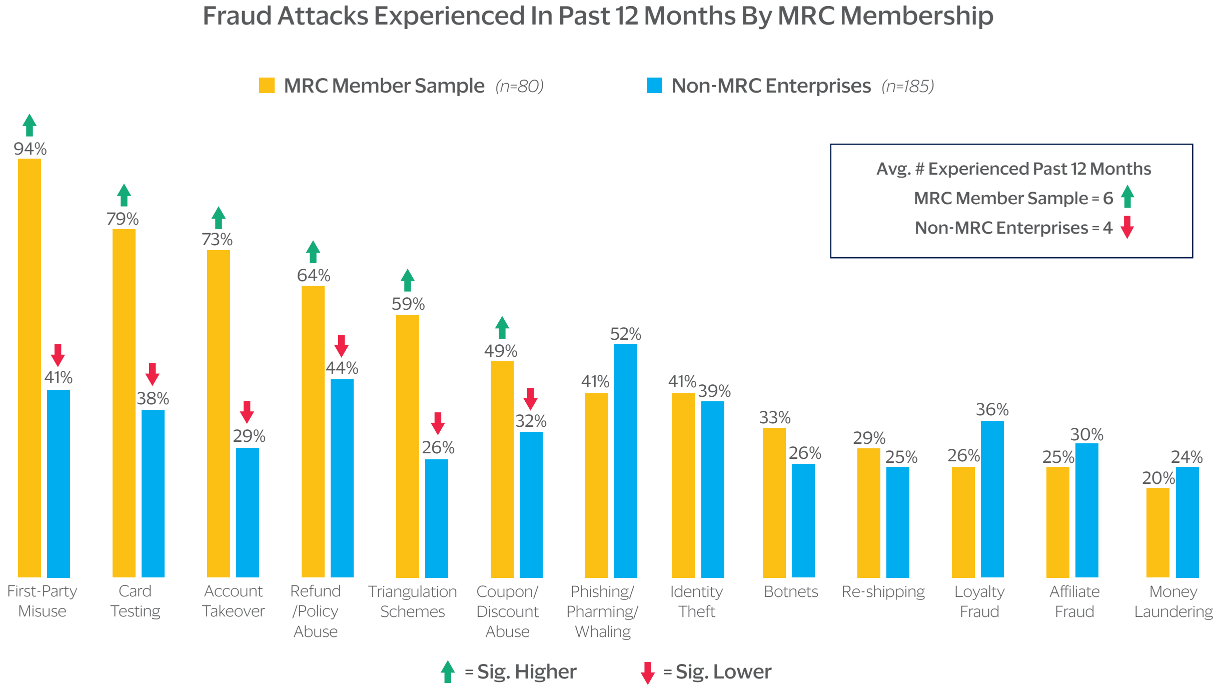
	Ranking By Region				Ranking By Company Size		
	N. America *(n=246)*	Europe *(n=84)*	Asia-Pacific *(n=95)*	Latin America *(n=74)*	SMB *(n=133)*	Mid-Market *(n=111)*	Enterprise *(n=255)*
1	Refund / Policy Abuse ↑	Refund / Policy Abuse	Phishing / Pharming / Whaling	Card Testing	Refund / Policy Abuse	Refund / Policy Abuse	First-Party Misuse ↑
2	First-Party Misuse ↑	First-Party Misuse	Refund / Policy Abuse ↓	Phishing / Pharming / Whaling	Phishing / Pharming / Whaling	First-Party Misuse	Refund / Policy Abuse
3	Phishing / Pharming / Whaling	Phishing / Pharming / Whaling	Loyalty Fraud	Identity Theft	Coupon / Discount Abuse	Identity Theft	Card Testing ↑
4	Card Testing	Card Testing	First-Party Misuse ↓	Account Takeover	First-Party Misuse ↓	Phishing / Pharming / Whaling	Phishing / Pharming / Whaling ↑
5	Identity Theft ↑	Coupon / Discount Abuse	Coupon / Discount Abuse	Refund / Policy Abuse ↓	Identity Theft	Loyalty Fraud	Account Takeover ↑
Avg. # Attacks Experienced In P12M	4.8 ↑	4.2	3.4 ↓	3.2 ↓	3.2 ↓	3.5 ↓	5.1 ↑

↑ = Sig. Higher vs. Other Segments ↓ = Sig. Lower vs. Other Segments

There are some differences by region and by company size when it comes to the most prevalent types of fraud impacting merchants over the past year (see Figure 21). North American merchants and enterprises report significantly higher rates of several types of fraud. In Asia-Pacific, phishing/pharming/whaling is the most widespread form of fraud, while in Latin America, card testing is the top threat.

Fraud also continues to be far more prevalent among MRC members, with this group averaging six different types of fraud experienced in the past year, versus four different types among non-MRC enterprises. Nearly 100% of MRC members surveyed this year say they experienced first-party misuse, and most were also hit by card testing, account takeover, refund/policy abuse and triangulation schemes, as well as coupon / discount abuse. Non-MRC enterprises are significantly less likely to report experiencing these attacks (see Figure 22).

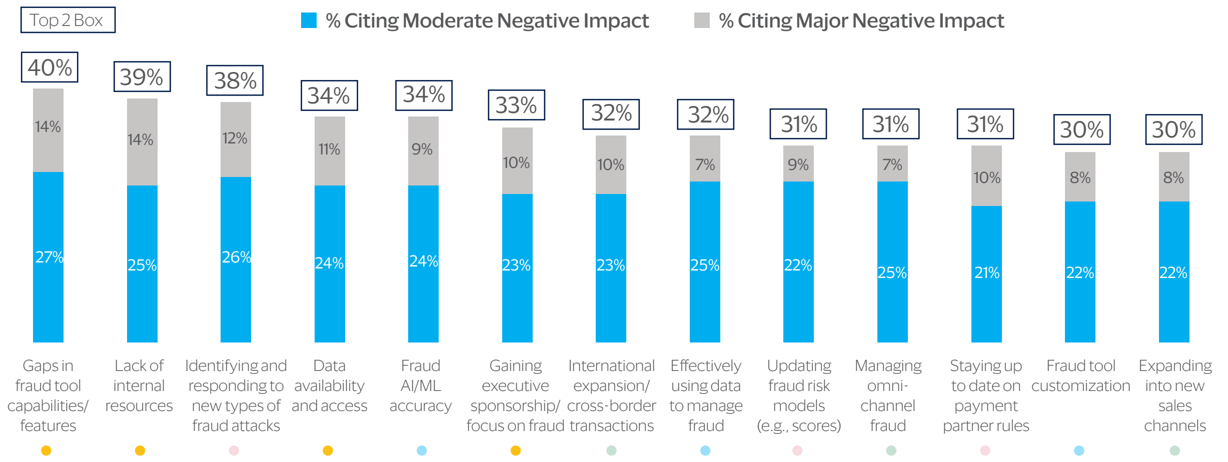
Figure 22: Fraud Attacks Experienced In Past 12 Months – By MRC Membership



Merchants Struggle With Resourcing And Operational Challenges In Their Efforts To Effectively Manage Fraud

Gaps and shortfalls in internal resources represent merchants' biggest overall challenge in fraud management. Globally, 30-40% of merchants identify gaps in fraud tool capabilities, lack of internal fraud management resources, and limited data access/availability as having significantly negative impacts on their abilities to manage fraud (see Figure 23).

Figure 23: Fraud Management Challenges



66% cite significant challenges with **internal resource constraints**

57% cite significant challenges with **staying up to date**

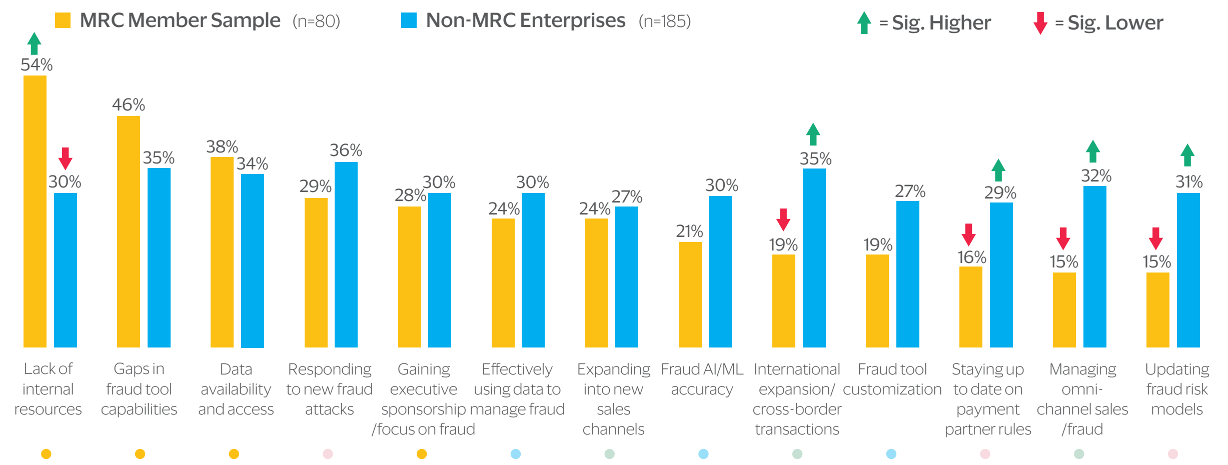
54% cite significant challenges with **managing fraud across channels & markets**

54% cite significant challenges with **leveraging data & tools effectively**

Staying up to date (on new attacks, risk models, and rule changes), managing fraud across different sales channels and geographic markets, and leveraging data and tools to effectively prevent and mitigate fraud are other high-level challenges inhibiting many merchants in their fraud prevention efforts (see Figure 23).

Fraud management challenges differ somewhat between MRC members and non-member enterprises. The former are primarily challenged by gaps and deficiencies in internal fraud management resources, e.g., lack of required data or gaps in fraud tool functionalities. Non-members are more challenged by the need to stay up to date on both emerging fraud attacks and on fraud-related rules and policies set forth by payment partners (see Figure 24).

Figure 24 – Fraud Management Challenges – By MRC Membership



↑ **75%** members vs. **58%** ↓ non-MRC enterprises internal resource constraints

43% members vs. **54%** non-MRC enterprises staying up to date

44% members vs. **51%** non-MRC enterprises managing fraud across channels & markets

45% members vs. **49%** non-MRC enterprises leveraging data & tools effectively

Fraud Makes A Major Dent In Merchant Businesses, Eroding Not Only Sales/ Revenues But Also Partner And Customer Relationships

Given the daunting range of fraud attacks and the sizable operational challenges outlined above, what kind of impact is fraud having on merchants' businesses?

Figure 25: Fraud Impact KPIs – Overall And By Region, Size Segment & MRC Membership

Fraud Impact KPIs *(Trimmed averages shown)*	**Overall**	**By Region**				**By Size**			**By MRC Membership**	
		North America	Europe	Asia Pacific	Latin America	SMB	Mid-Market	Enterprises	MRC Sample	Non-MRC Enterprises
Fraud Rate By Revenue (% of total annual eCommerce revenue lost to payment fraud globally)	**3.1%**	2.8%	3.5%	3.3%	2.7%*	3.7%	4.1%	2.3%	0.6	3.9%
Fraud Rate By Order (% accepted orders in past 12 months that turned out to be fraudulent)	**3.3%**	3.6%	2.8%	3.6%	3.4%*	4.3%	3.7%	2.6%	0.6%	4.0%
Order Rejection Rate (% eCommerce orders rejected due to suspicion of fraud in past 12 months)	**5.8%**	6.5%	4.3%	5.5%	6.0%	6.2%	5.1%	5.9%	3.3%	7.5%
Chargeback / Dispute Win Rate (annual % of fraud-coded chargebacks & disputes won by the merchant)	**17.4%**	20.8%	10.3%	15.6%	16.6%	16.6%	15.0%	18.8%	28.0%	16.0%

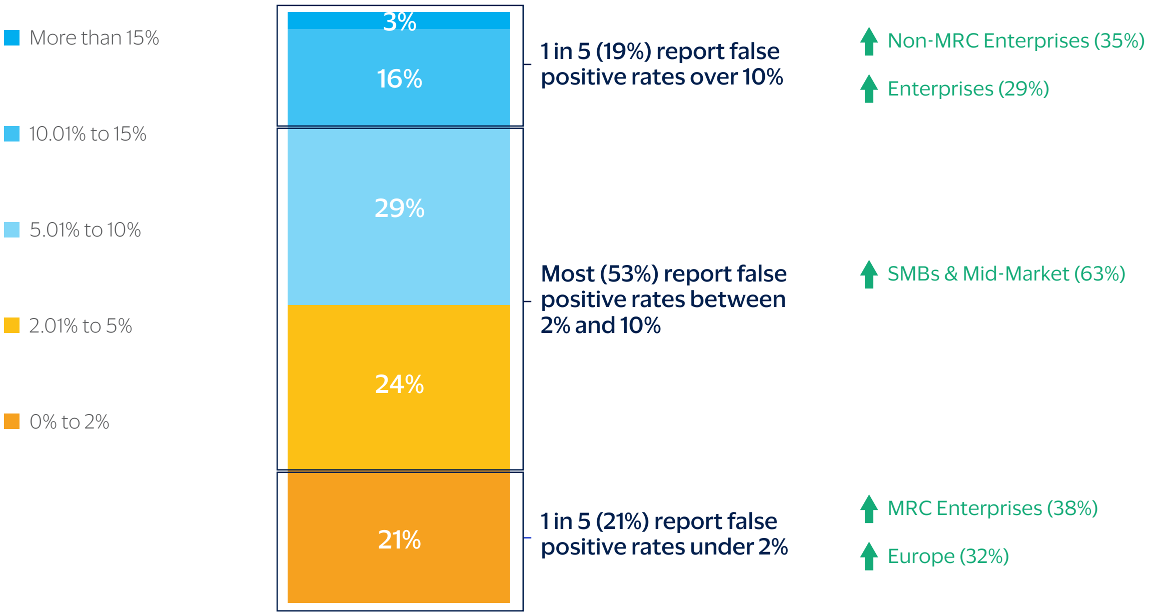
*Low Base (n<30) 🟩 = Sig. Better vs. Other Segments 🟥 = Sig. Worse vs. Other Segments

Several fraud metrics collected in this year's survey suggest the negative impact of fraud is considerable: Merchants estimate the share of total eCommerce revenue lost to payment fraud to be 3% annually, skewing higher in Europe and APAC as well as for SMB and midsize merchants (see Figure 25).

Merchants also report that roughly 3% of their accepted eCommerce orders turn out to be fraudulent, a figure that skews higher for North American merchants, SMBs, and non-MRC enterprises. In addition, merchants say they reject around 5% of orders due to suspicions of fraud, a figure that also skews upward for North American merchants and non-MRC enterprises. Globally, dispute win rates sit below 20%, with merchants in Europe citing a far lower win rate of approximately 10%.

In addition to the negative impacts quantified in Figure 25, fraud also frays merchant relationships with both customers and commercial partners. One indicator of this is the number of "customer insults," or false positives, that merchants experience on eCommerce orders. Figure 26 shows most merchants cite false positive rates between 2% and 10% of total eCommerce orders, however, one in five report rates above 10%, a figure that skews significantly higher for Non-MRC enterprises and enterprises, in general.

Figure 26: Rate Of False Positives Or "Customer Insults"



**Not shown in chart: 6% selecting Don't Know or Prefer Not To Say*

↑ = Sig. Higher vs. Other Segments

Overall, these metrics paint a vivid picture of the substantial harm fraud inflicts on merchants' businesses, both in terms of eCommerce sales and revenues, as well as conflicts and tensions with customers and commercial partners.

5. First-Party Misuse

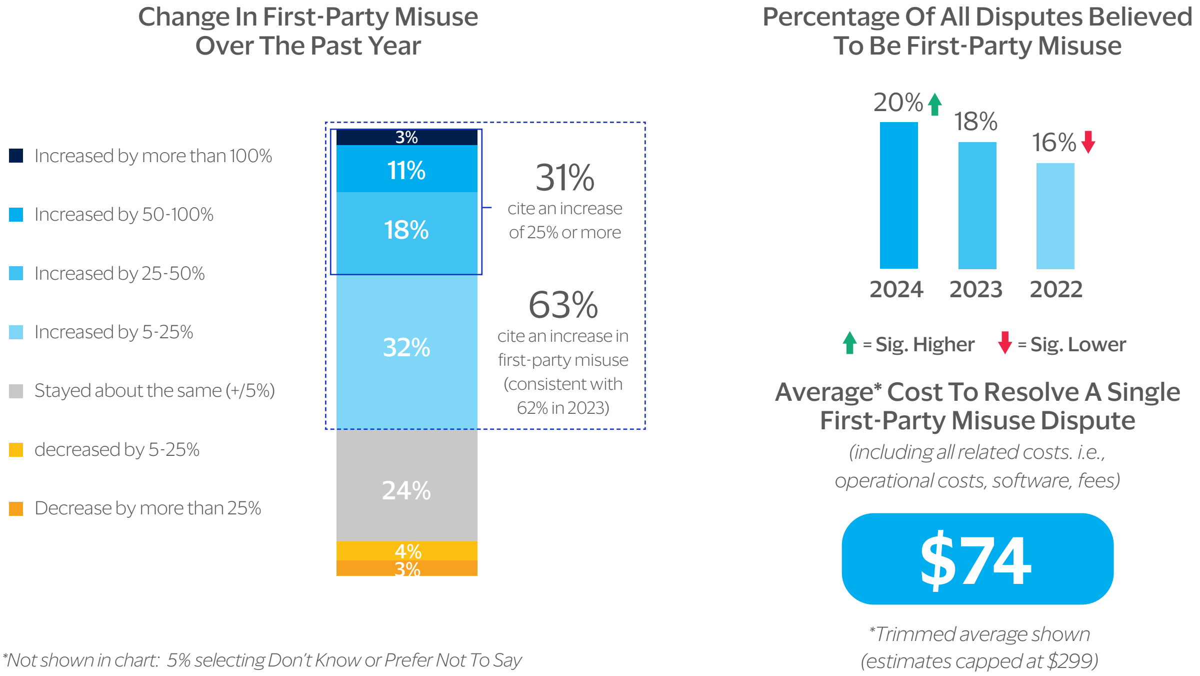
As merchants have grappled with a rise in first-party misuse (or FPM) in recent years, it has become clear that payment and fraud professionals are in need of fresh, detailed insights on this particularly harmful form of fraud. To help deliver such insights, this year's survey includes an extensive set of questions about the trend of increasing FPM, what merchant fraud professionals view as the major causes and costs of this trend, and what strategies and tactics they are employing to counter it. This section delves directly into the results of these questions to paint a vivid picture of the state of FPM.

First-Party Misuse Continues To Skyrocket, Especially Among Merchants In North America As Well As Mid-Market And Enterprise Merchants

To begin, it is important to underscore that FPM is not just ticking upward but, at least according to the majority of merchants, rising rapidly.

For the second consecutive year, more than 60% of merchants in the survey say they experienced an increase in FPM over the past 12 months (see Figure 27). Even more striking, half of those citing an increase (31% globally) estimate that the incidence of FPM increased 25% or more compared with the prior year. This finding is further substantiated by the significant increase in the percentage of all fraudulent disputes that merchants attribute to FPM, which has risen from 16% in 2022 to 20% this year. For a large share of merchants, it is clear that FPM is rising not just incrementally but exponentially.

Figure 27: Change In First-Party Misuse, Share Of Disputes Attributed To FPM & Average Cost To Resolve An FPM Dispute



*Not shown in chart: 5% selecting Don't Know or Prefer Not To Say

*Trimmed average shown (estimates capped at $299)

While the rise in first-party misuse is being felt by merchants across the board, there are some segments that seem to be bearing the brunt of it—namely merchants in North America as well as midsize and enterprise merchants. The data table in Figure 28 supports this notion, showing that merchants in these segments were more likely to cite sizable increases in FPM rates over the past year.

Figure 28: Change In First-Party Misuse – By Region, Size Segment & MRC Membership

Change In First-Party Misuse Over The Past Year	**2024**	**Region**				**Merchant Size**			**Membership**	
		North America	Europe	Asia Pacific	Latin America	SMB	Mid-Market	Enterprises	MRC Sample	Non-MRC Enterprises
Base	*1,166*	*494*	*243*	*267*	*162*	*352*	*269*	*545*	*147*	*1,019*
NET % CITING ANY INCREASE	**63%**	**69%**	**59%**	**60%**	**57%**	**55%**	**64%**	**68%**	**46%**	**76%**
Iincreased by more than 100%	**3%**	3%	2%	4%	1%	2%	3%	3%	2%	4%
Increased by 50-100%	**11%**	10%	10%	12%	10%	10%	12%	10%	7%	12%
Increased by 25-50%	**18%**	24%	14%	13%	13%	11%	18%	22%	12%	26%
Increased by 5-25%	**32%**	32%	32%	31%	33%	33%	30%	32%	26%	35%
Stayed about the same (+/- 5%)	**24%**	21%	30%	22%	27%	30%	27%	18%	27%	16%
Decreased by more than 5%	**7%**	4%	7%	10%	14%	9%	7%	6%	5%	7%
Don't know / we do not track OR Prefer not to say	5%	6%	5%	8%	2%	6%	2%	7%	22%	2%

🟩 = Sig. Better vs. Other Segments 🟥 = Sig. Worse vs. Other Segments

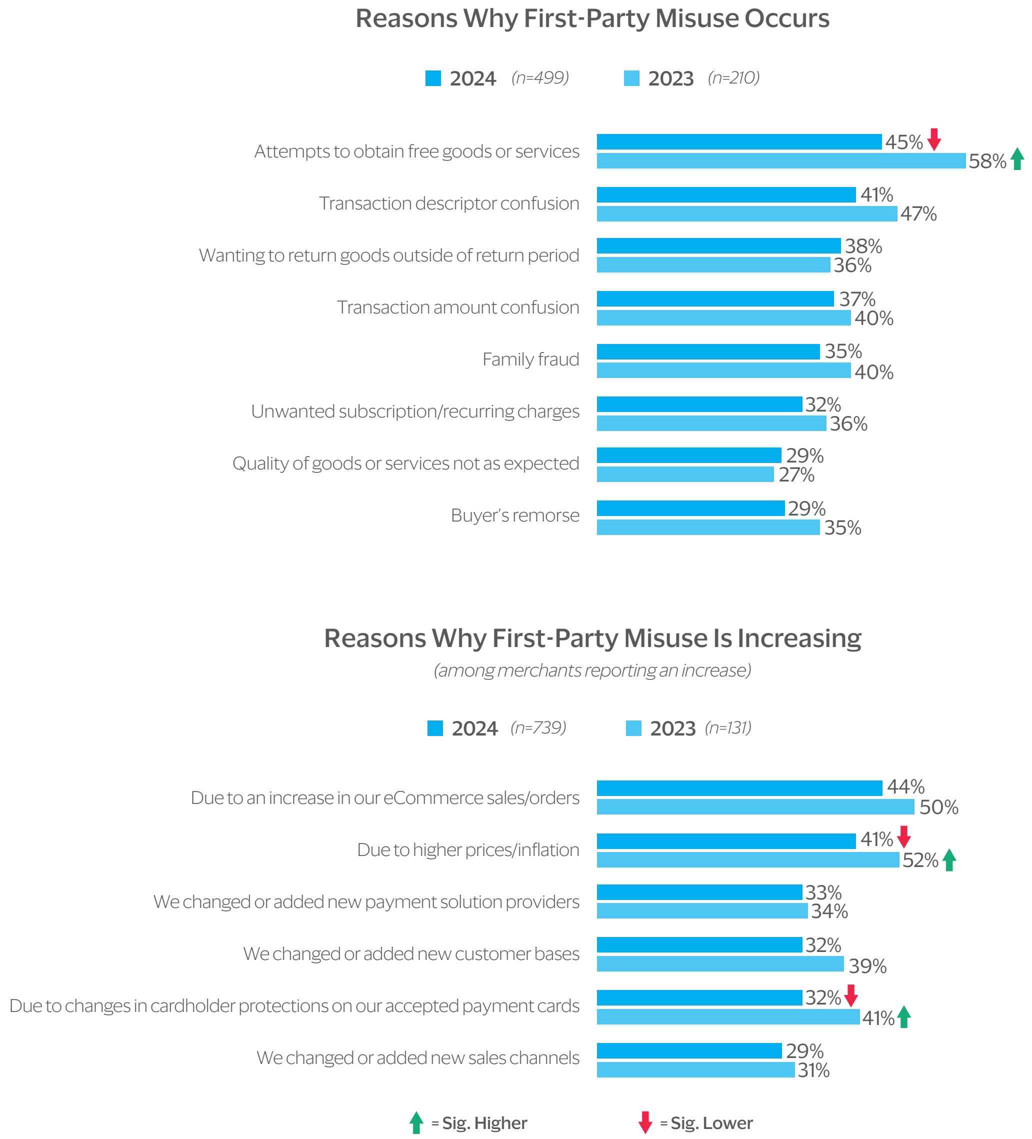
Additionally, there is a significant difference in reported change in FPM between MRC members and non-MRC enterprises, with a far greater share of the latter group reporting major increases in FPM over the past year. But it is worth noting that 22% of MRC members did not provide an answer to this question, so this difference should be taken skeptically, statistically speaking.

In addition to answering questions about the change and costs of FPM, merchants also offered insight in the survey about drivers of this form of fraud, both in general and specific to the rapid increase merchants have witnessed in recent years.

To the first point, merchants identify a range of likely reasons why FPM occurs in general (see Figure 29). Obviously, attempts to obtain free goods or services is a major reason why customers would engage in this type of fraud. This, along with most other reasons shown, such as wanting to return goods outside of return periods and unwanted subscriptions or recurring charges, represents a set of "bad faith" motivations that drive consumers to intentionally exploit merchant return policies in a fraudulent way. The reality is that merchants will always struggle to prevent FPM attempts driven by these bad faith rationales, and they will need to try to recoup such losses through dispute mechanisms after the fact.

But in addition to those drivers, each selected by at least one-third of merchants in this year's survey, there are other motivations that are rooted in consumer confusion, not bad faith—for instance, confusion about transaction descriptors or amounts on a customer's card statement. Merchants do have an opportunity to work proactively with card issuers and other financial partners to help mitigate these drivers—for instance, by providing consumers with clearer, more detailed, and more accurate transaction information. Such efforts, if successful, should have a material impact in tamping down this spike in FPM.

Figure 29: Reasons Why FPM Occurs & Reasons Why It Is Increasing (2023-2024)



Note: Other reasons suggested by merchants include increasing consumer awareness of what first-party misuse is and how to successfully perpetrate it, increasing sharing of first-party misuse tips and practices online (social media, etc.), and the emergence of fraud-as-a-service.

Merchants also offered opinions on why FPM has been rising so rapidly, with the results displayed in the chart at the bottom of Figure 29. Compared with last year, merchants were less likely to highlight inflation/higher prices as the number one cause, although many still see this as a major driver of the trend. They were also significantly less likely to blame changes in cardholder protections this year than last year. Instead, there is a similar pattern to the chart above, with merchants attributing this spike to multiple factors, like overall increases in eCommerce sales/orders and changes in payment providers, sales channels, or customer bases.

Notably, many merchants opted to write in additional, open-ended answers at this survey question. The key themes from those responses are summarized underneath the chart. These include speculations that increasing consumer awareness of FPM, combined with increased sharing of FPM tips and practices online (including those tied to the emergence of fraud-as-a-service), are all exacerbating this trend. Several verbatim comments offered by merchants here are displayed in Figure 30. To sum up, while there are obviously multiple factors driving FPM in general, merchants do have suspicions about new and worrisome factors potentially worsening the recent rise in this form of fraud.

Figure 30: Reasons For Increasing First-Party Misuse... In Merchants' Words

> "People are learning how to game the system."
> *- MRC Member*

> "Increase in fraud services online."
> *- MRC Member*

> "Likely due to 'social media hacks' with people sharing ways to cheat businesses and reasoning that it is okay since we as businesses are 'wealthy' or 'protected.'"
> *- Enterprise Merchant*

> "Customers are more aware of chargeback options and fraud-as-a-service is more prevalent."
> *- MRC Member*

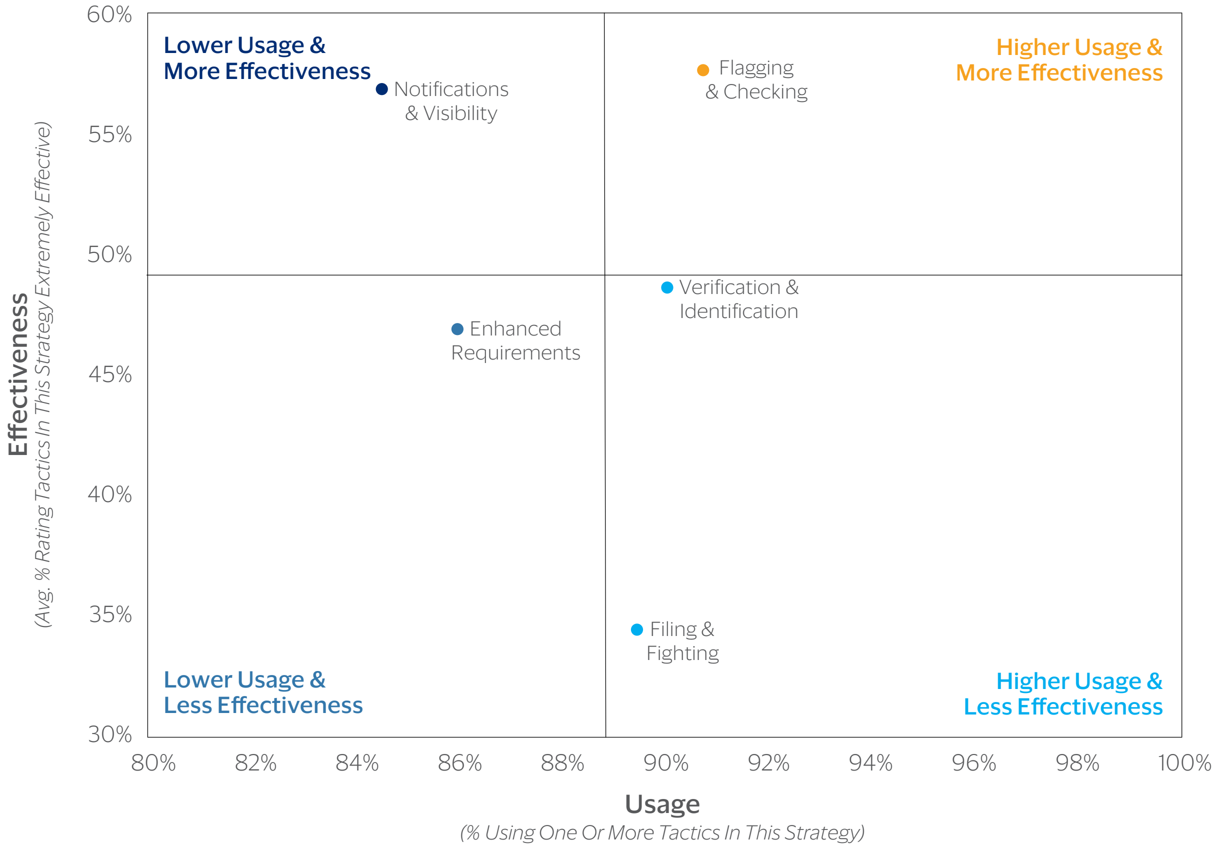
> "We changed our refund policy to make it easier for the customer, and therefore, easier to take advantage of for unethical people."
> *- Enterprise Merchant*

> "It seems that the issuing banks allow almost every dispute to be submitted."
> *- MRC Member*

Obviously, FPM is a major issue for merchants right now. So, the next question is, what are they doing about it? To answer this, the survey probed both the high-level, strategic approaches and the tactical tools and techniques that merchants are employing to counter this growing threat.

At a high level, merchants are leveraging multiple strategic approaches in their attempts to combat FPM in a variety of different ways. In Figure 31, the survey data has been aggregated to display the relative usage and effectiveness of five different strategic approaches. As indicated by the relatively close clustering of all five approaches on the x-axis, each strategic approach is being used by the vast majority of merchants worldwide. In other words, the vast majority of merchants are attacking this problem from all or most angles possible.

Figure 31: Usage Vs. Effectiveness Of Strategic Approaches To Combat First-Party Misuse

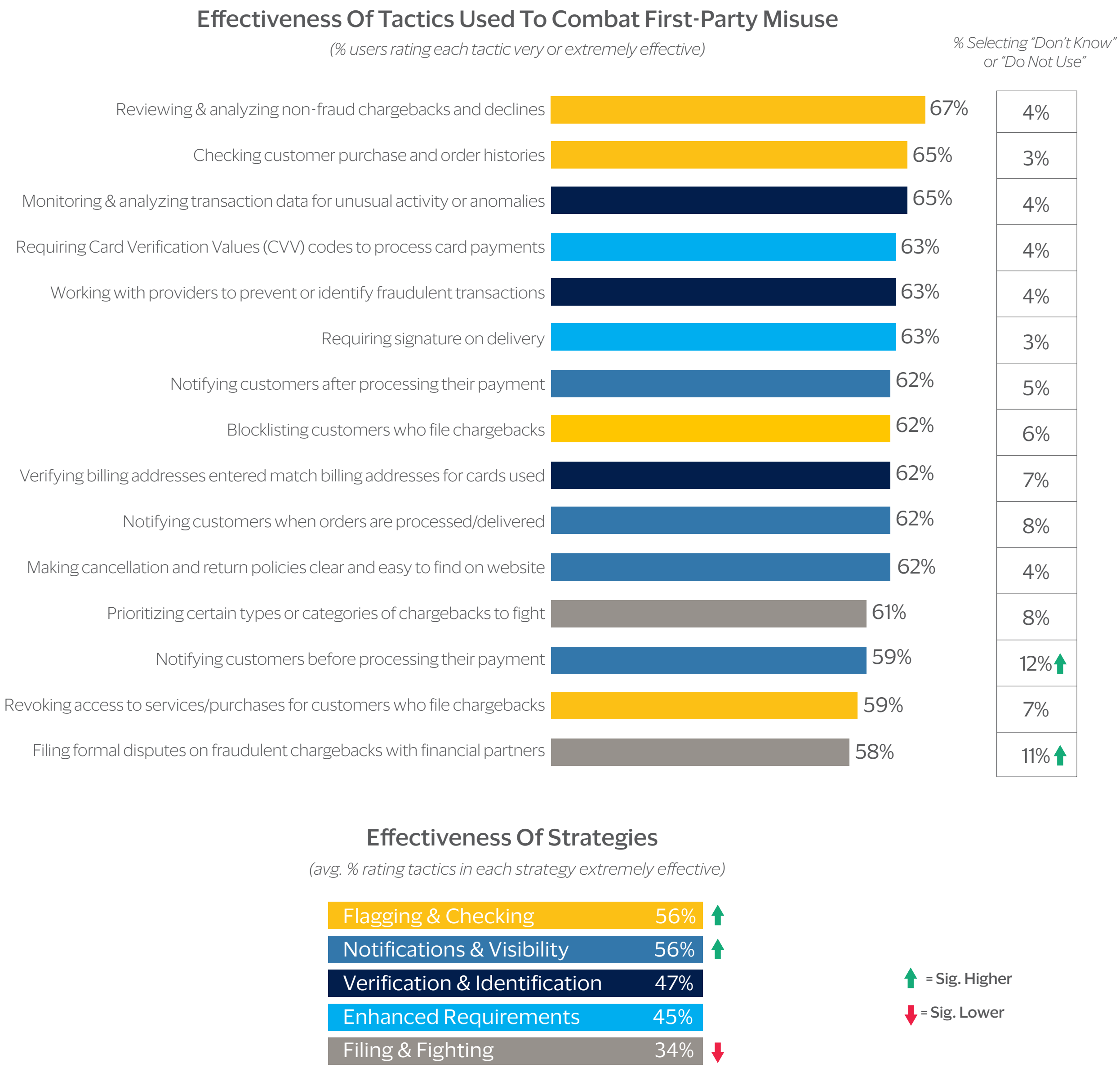


Where there is greater differentiation between strategies is on the y-axis, i.e., their relative effectiveness. Scanning from top to bottom reveals that the most effective strategic approach—flagging & checking—is also the most widely used. But the second most effective—notifications & visibility—is actually the least widely used. This highlights a potential opportunity for merchants to make more headway in countering FPM by applying and enhancing notification and visibility tactics, such as making refund and return policies clear, detailed, and hard to miss for online shoppers and consumers.

Another notable data point is the relative ineffectiveness of filing & fighting strategies. Despite being used by nine out of 10 merchants, less than 35% rate filing & fighting measures extremely effective in countering FPM. So as merchants consider leaning into other tactics and strategies, they may be able to reduce time and resources spent in that area without suffering much incremental damage, in terms of increased impacts and losses from FPM.

Given these insights about the general approaches merchants are using to combat FPM, what specific tactics, tools, and techniques are merchants employing to execute these strategies? This information is provided in Figure 32. These data show merchants view reviewing and analyzing non-fraud chargebacks as the most effective single tactic for countering FPM, closely followed by checking customer purchase and order histories and monitoring transaction data for unusual patterns. Requiring CVV values to process card payments and working with providers to jointly prevent or identify fraudulent transactions round out the top five.

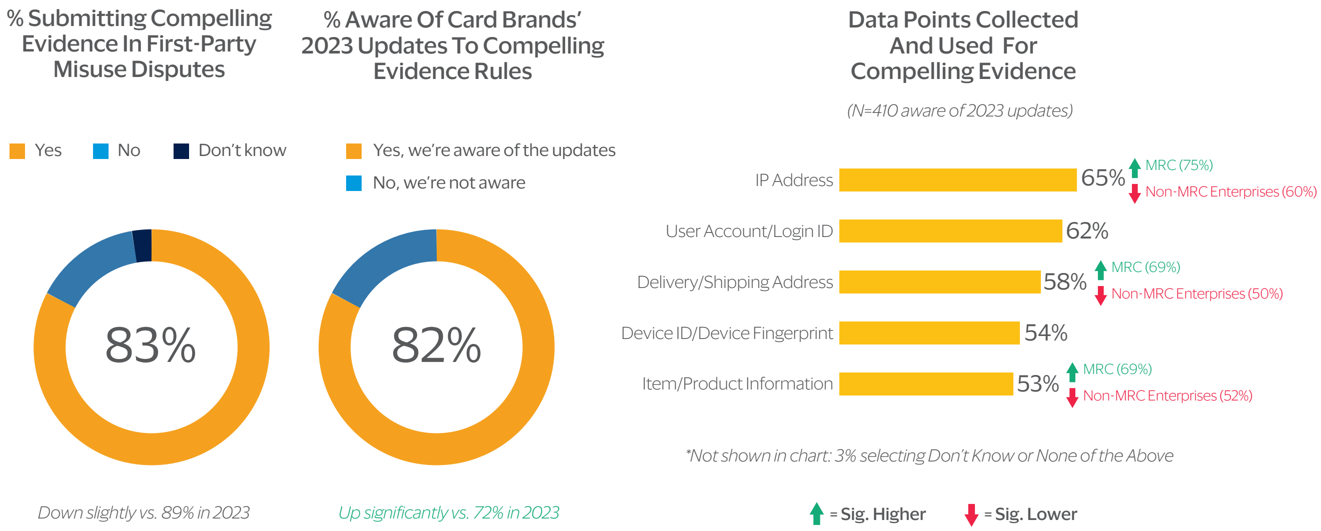
Figure 32: Effectiveness Of Strategies And Tactics To Combat First-Party Misuse



Again, these data underscore the importance of pulling multiple tactical levers to combat FPM, as the top five most effective tactics span three different strategic approaches and the gap between the most effective and least effective tactic is less than 10%. The table below the chart depicts which tactics fall under each strategy, while also indicating once more that the top two most effective strategies of flagging & checking and notifications & visibility are seen by merchants to have a significantly greater impact on reducing FPM, compared to “fighting & filing.”

The final set of insights in this section center around the usage and perceptions of compelling evidence when merchants are disputing FPM transactions with card issuers. Globally, more than eight in 10 merchants (83%) submit compelling evidence in first-party misuse disputes, and a similar share are aware of the major updates card networks made to compelling evidence policies during 2023 (see Figure 33).

Figure 33: Awareness & Usage Of Compelling Evidence In FPM Disputes


% Submitting Compelling Evidence In First-Party Misuse Disputes

% Aware Of Card Brands' 2023 Updates To Compelling Evidence Rules

Data Points Collected And Used For Compelling Evidence

(N=410 aware of 2023 updates)

Not shown in chart: 3% selecting Don't Know or None of the Above

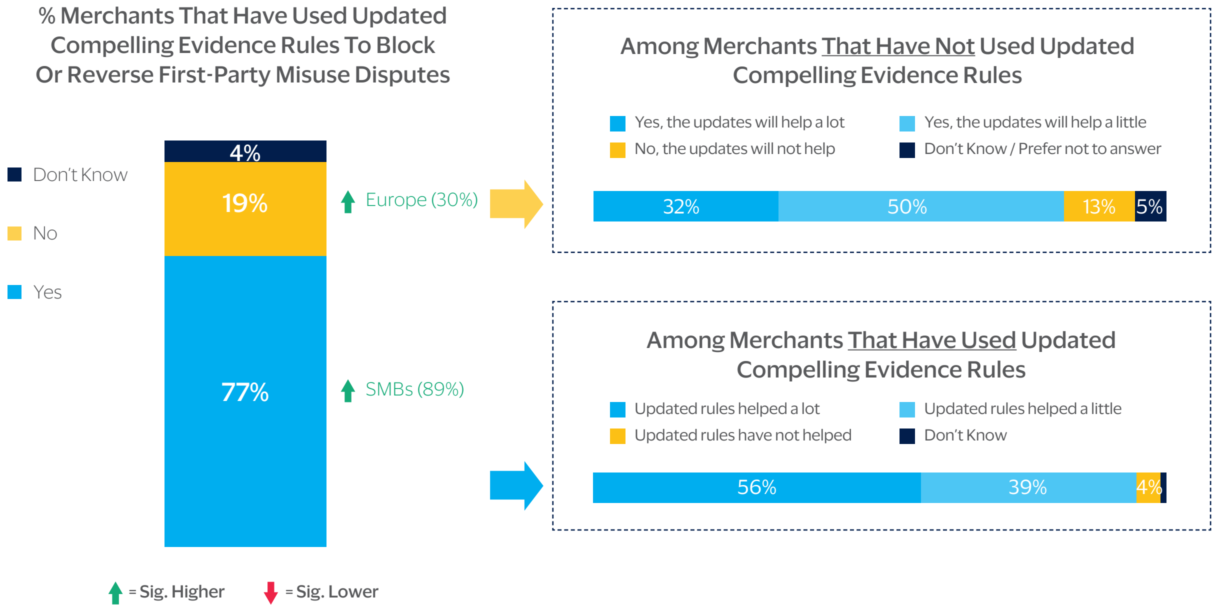
Down slightly vs. 89% in 2023

Up significantly vs. 72% in 2023

In addition to these high levels of usage and awareness, this graphic shows the share of merchants collecting various data points that are relevant to submit as compelling evidence. The data show that most merchants using compelling evidence collect and submit each of these five data points, however these majorities are relatively slim, with 35% to 47% of merchants not selecting each one.

Many merchants, therefore, have an opportunity to increase the share of disputes they win with compelling evidence, if they can collect and submit more of the relevant data points (where such data is available and relevant). Also, it is notable that MRC members are more likely than non-member enterprises to leverage a few of these key data points, suggesting the former group may be having more success in using compelling evidence to counter FPM.

Figure 34: Usage & Perceptions Of Card Brands' Updated Compelling Evidence Rules



And when it comes to the updates major card brands made to compelling evidence rules in 2023, slightly more than three-quarters (77%) of merchants report successfully blocking or reversing an FPM-related dispute using these rules (see Figure 34). SMBs over-index on having successfully applied these new rules, while merchants in Europe under-index significantly. Among all merchants—both those who have and have not used the updated rules—there is a general belief that these updates will be helpful in resolving such disputes. And this positive sentiment is much stronger among merchants who have already made use of the updated rules, indicating that merchants are indeed recognizing the additional benefits they expect from the updated compelling evidence policies.

In total, the insights in this section illustrate that FPM is certainly a pressing, growing problem for merchants. But they have a range of strategic and tactical tools they can apply to help mitigate it, including making full use of the current compelling evidence rules in cooperation with card issuers and other payment and fraud solution providers.

6. Fraud Management

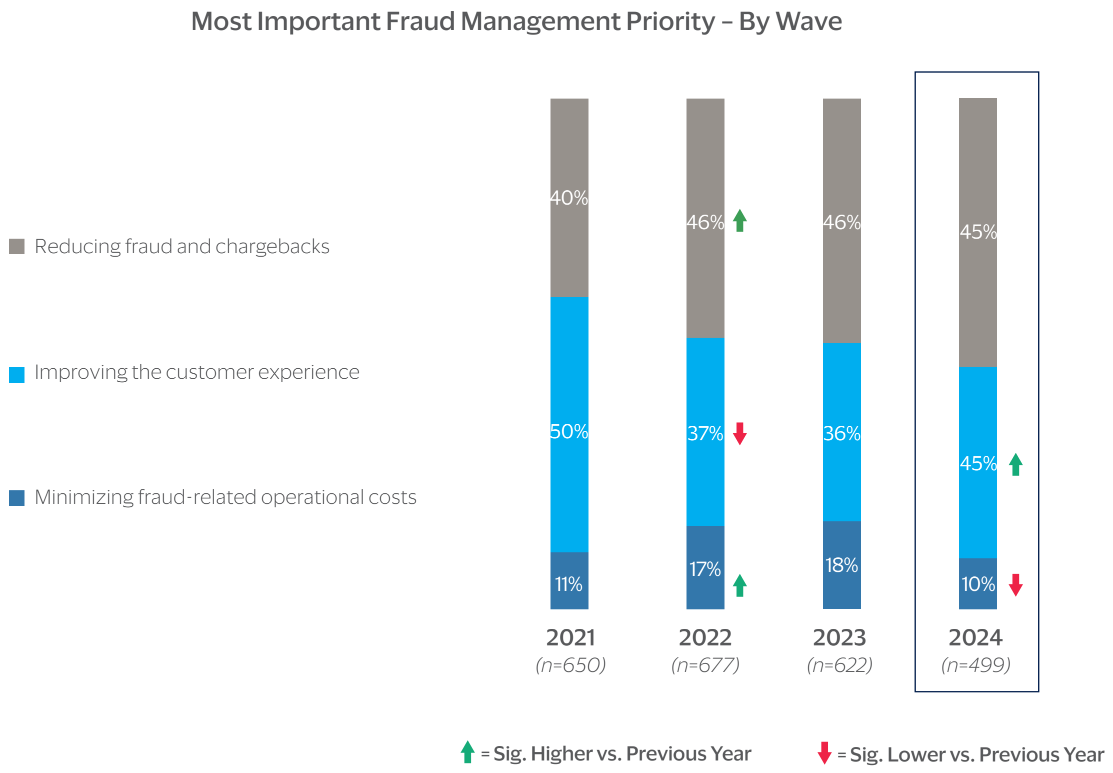
In this section of the report, the focus shifts to the general strategies and tactics merchants are employing to manage and mitigate payment fraud. Specifically, this section examines the most important fraud management priorities for merchants and identifies the main areas of improvement and investment merchants plan to focus on over the next year.

This section also explores merchant approaches to manual versus digital fraud screening and usage of various fraud prevention tools and techniques, including those powered by artificial intelligence (AI) and machine learning (ML).

Merchants Take Divergent Paths On Fraud Strategy And Spending

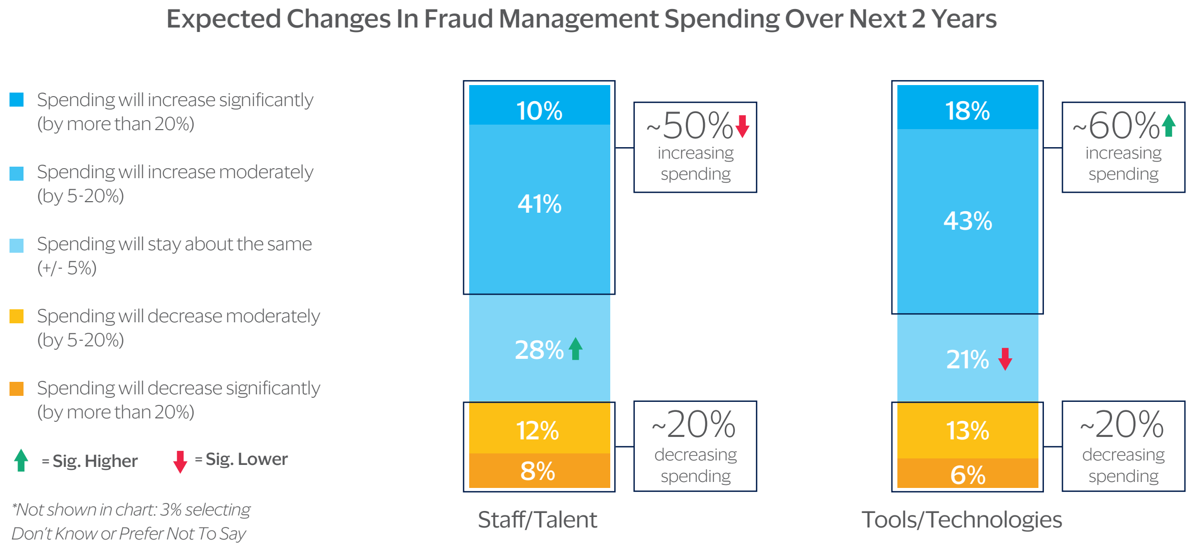
At a strategic level heading into 2024, fewer merchants are prioritizing minimizing operational costs as the key imperative driving their fraud management strategies. But they seem to be equally split, now, on prioritizing improving the customer experience and reducing fraud and chargebacks (see Figure 35).

Figure 35: Top Fraud Management Priority (2021-2024)



Similarly, around half of merchants plan to increase spending on fraud management tools/technologies and staff/talent over the next two years, but the other half are intent on either doing more with their current spending levels or on finding ways to reduce investment while maintaining or increasing performance (see Figure 36). Overall, merchants are slightly more likely to ramp up spending on tools and technologies than staff and talent.

Figure 36: Expected Change In Fraud Management Spending Over Next 2 Years



Spending plans differ significantly by region and size segment, suggesting merchants playing in similar markets may be taking similar approaches, even as their path diverges from those in other regions or revenue tiers. Regionally, merchants in North America and APAC are most likely to ramp up spending on both fraud management staff and tools/ technologies, whereas those in Europe and Latin America are more apt to keep budgets for these areas flat or decrease them (see Figure 37 and Figure 38).

Figure 37: Expected Change in Spending On Fraud Management Staff/Talent – By Region & Size Segment

Expected Change In Spending On Fraud Management Staff/ Talent in Next 2 Years	**Overall**	**By Region**				**By MRC Membership**		
		North America	Europe	Asia Pacific	Latin America	SMB	Mid-Market	Enterprise
Base	*253*	*134*	*53*	*36*	*30*	*70*	*65*	*118*
NET % EXPECTING ANY INCREASE	**51%**	**58%**	**42%**	**53%**	**33%**	**40%**	**46%**	**60%**
% Expecting Significant Increase (>20%)	10%	14%	0%	17%	3%	3%	6%	17%
% Expecting Moderate Increase (5-20%)	41%	44%	42%	36%	30%	37%	40%	43%
% Expecting Same (Flat) Spending (+/- 5%)	28%	26%	36%	33%	13%	29%	28%	27%
% Expecting Moderate Decrease (5-20%)	12%	10%	15%	6%	27%	14%	17%	8%
% Expecting Significant Decrease (>20%)	8%	6%	8%	6%	23%	16%	9%	3%
NET % EXPECTING ANY DECREASE	**21%**	**16%**	**23%**	**11%**	**50%**	**30%**	**26%**	**12%**

🟩 = Sig. Higher vs. Other Segments 🟥 = Sig. Lower vs. Other Segments

When it comes to size segments, SMBs and mid-market merchants are more likely to decrease budgets for staff / talent, in particular, whereas most enterprises plan to raise spending on fraud management personnel (see Figure 37).

Figure 38: Expected Change In Spending On Fraud Management Tools/Technologies – By Region & Size Segment

Expected Change In Spending On Fraud Management Tools & Technologies In Next 2 Years	Overall	By Region				By MRC Membership		
		North America	Europe	Asia Pacific	Latin America	SMB	Mid-Market	Enterprise
Base	*253*	*134*	*53*	*36*	*30*	*70*	*65*	*118*
NET % EXPECTING ANY INCREASE	**60%**	**67%**	**42%**	**75%**	**47%**	**56%**	**55%**	**66%**
% Expecting Significant Increase (>20%)	18%	21%	6%	31%	10%	17%	12%	21%
% Expecting Moderate Increase (5-20%)	43%	46%	36%	44%	37%	39%	43%	45%
% Expecting Same (Flat) Spending (+/- 5%)	21%	19%	38%	6%	17%	17%	28%	19%
% Expecting Moderate Decrease (5-20%)	13%	10%	15%	8%	23%	16%	12%	11%
% Expecting Significant Decrease (>20%)	6%	4%	6%	8%	10%	10%	5%	3%
NET % EXPECTING ANY DECREASE	**18%**	**14%**	**21%**	**17%**	**33%**	**26%**	**17%**	**14%**

🟩 = Sig. Higher vs. Other Segments 🟥 = Sig. Lower vs. Other Segments

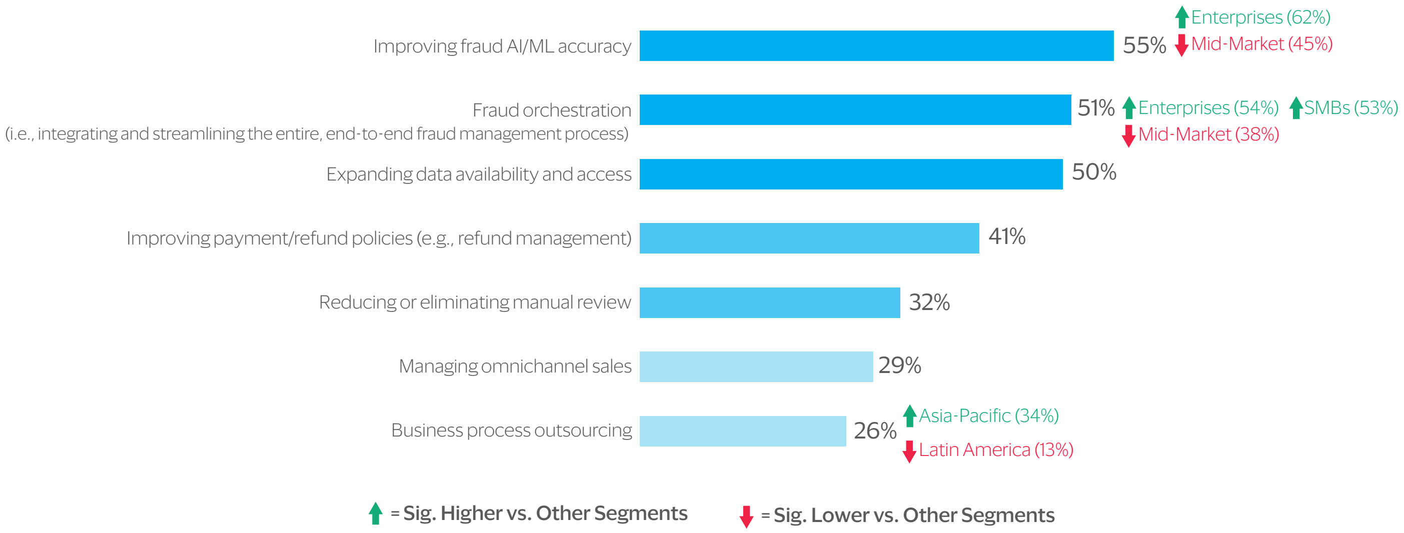
Enhancing Fraud Tools, Improving Fraud Orchestration And Improving Payment/Refund Policies Are Top Areas For Improvement

Merchants show more consensus when it comes to which aspects of fraud management they will focus on improving over the next year, with the majority citing AI/ML-driven fraud management tools, fraud orchestration, and refund management as top priorities (see Figure 39). Business process outsourcing, managing omnichannel sales, and reducing or eliminating manual review are less likely to be points of emphasis, with less than a third of merchants identifying these as priority areas for improvement next year.

The focus on improving payment and refund policies is likely, in part, driven by the rise of FPM and refund/coupon abuse, illustrated by the data reported in sections four and five above.

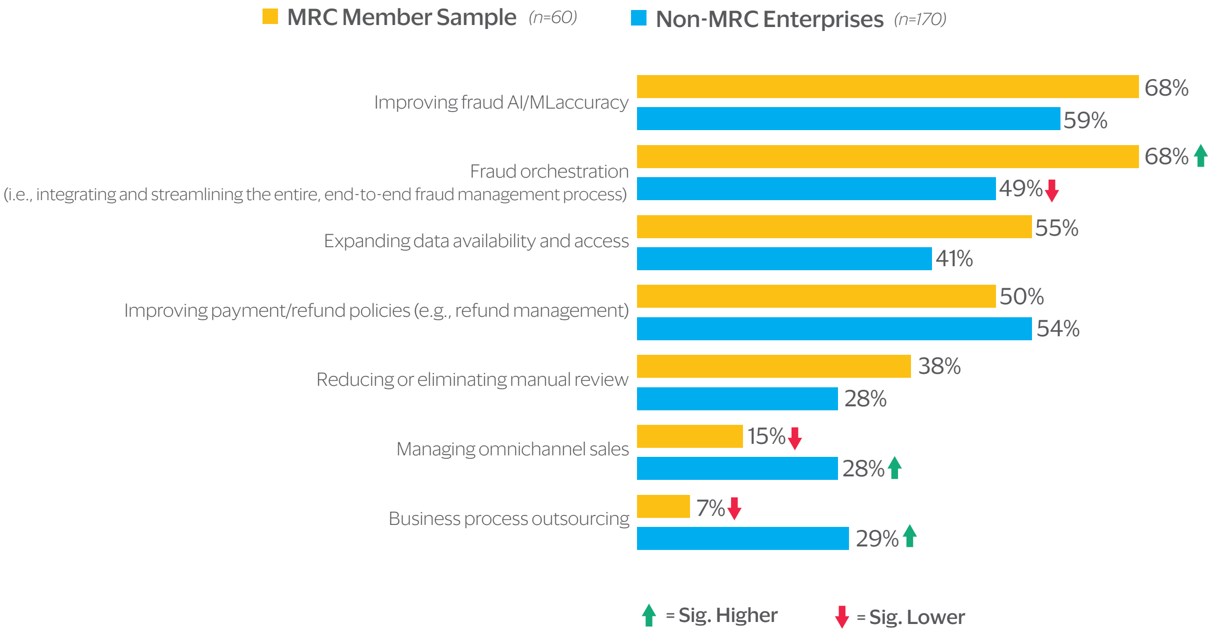
Enterprises are especially likely to say that improving fraud AI/ML accuracy and improving payment/refund policies are areas of improvement (with SMBs also more likely to focus on this area), while midsize merchants are far less likely to focus on these areas when improving fraud management moving forward.

Figure 39: Top Improvement Areas For Fraud Management Over The Next 12 Months (2024)



MRC members cite distinct areas for improvement they plan to focus on over the next year compared with non-MRC enterprises (see Figure 40). MRC merchants are especially likely to focus on improving AI/ML accuracy, fraud orchestration, and data availability/access, while non-members are more concerned with better managing omnichannel sales and improving their approach to business process outsourcing.

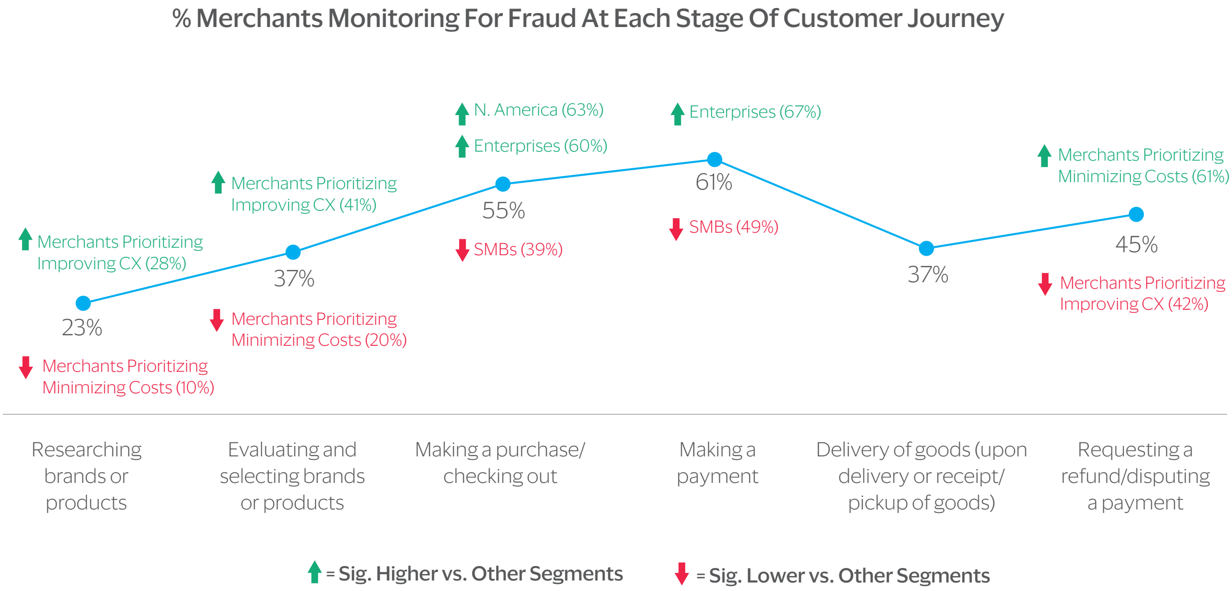
Figure 40: Top Improvement Areas For Fraud Management – By MRC Membership



Merchants Are Also Acting Differently At The Tactical Level, Although Virtually All Seem Intent On Adopting AI-Driven Tools & Techniques

When it comes to tactical tools and technologies merchants use to manage and prevent fraud, more than half make use of these to monitor and signal potential fraud at the purchase and payment stages of the customer journey. But most do not monitor fraud at pre- or post-purchase stages, including refund requests or disputes (see Figure 41).

Figure 41 – Fraud Monitoring Throughout The Customer Journey



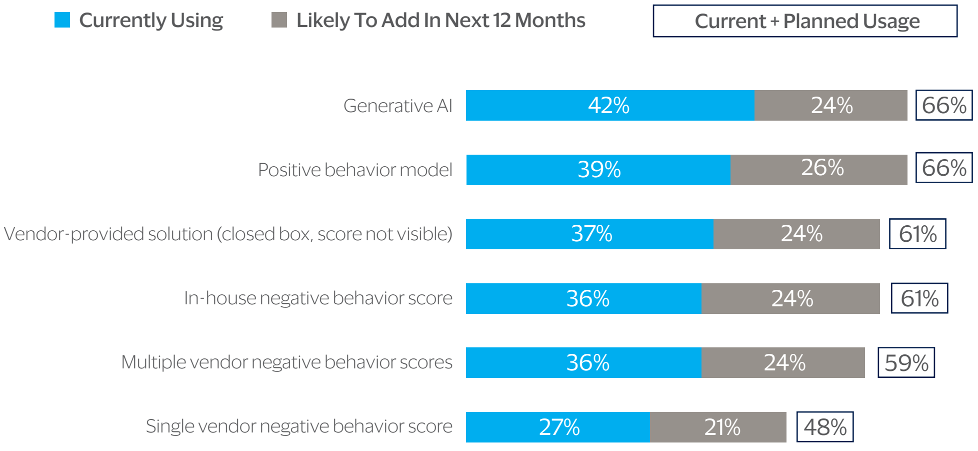
This may be one of the 'gaps in fraud tool functionalities' many merchants cite as a key challenge at the strategic level. There are some differences in fraud monitoring by merchant segment, as enterprises are more likely, and SMBs less likely, to screen during the payment stage. North American merchants are also more likely to use a tool or signal to identify potential fraud during the making a purchase/checking out stage.

Also, merchants prioritizing improving CX as their primary imperative in fraud management are significantly more likely to monitor at pre-purchase stages, while those prioritizing minimizing costs are more apt to monitor at the post-purchase stage of refunds and disputes.

Merchants Aim To Increase Adoption Of AI/ML-Driven Fraud Tools

When it comes to specific tools and techniques merchants are employing to monitor and prevent fraud across the customer journey, this year's survey focuses on tools driven by AI and/or ML.

Figure 42: Current + Planned Usage Of AI/ML-Driven Fraud Management Tools



**Not shown in chart: 3% selecting Don't Know or Prefer Not To Say*

Globally, merchants are using an average of one to two different AI/ML-driven fraud management tools; however, as shown in Figure 42, none of the six tools tested in the survey is currently in use by more than 50% of merchants. But adoption of these tools is likely to grow swiftly, as predicted usage rates for five out of six tools shown in this figure sit above 50% when factoring in the share of merchants who expect to add them in the next 12 months. No doubt, these advanced solutions will quickly become central tools in merchants' anti-fraud toolkits as they are implemented and integrated into their IT systems over the coming months.

Conclusion

Altogether, the themes and findings in this year's report illustrate the complex, constantly evolving challenges facing eCommerce merchants as they look to refine their strategic approaches to payments and fraud and to execute those strategies successfully via tactical tools and techniques.

Regarding payments, merchants continue to expand acceptance offerings while recognizing that, as more customers make use of new payment methods like real-time payments, these methods will become increasingly attractive targets for fraudsters to try to exploit. Merchants also continue to utilize multiple tools, techniques, and practices to provide customer-friendly payment experiences and to ensure smooth, secure, and profitable payment processing. These include encouraging customers to pay with certain methods, employing various tools and techniques to increase payment authorization rates, and leveraging tokenization to improve security when processing payment and customer data.

As payment methods, types of payment fraud, and payment management tools and techniques continue to proliferate, merchants are feeling pressure to track and analyze a growing array of payment-related metrics. Ensuring a consistent and coherent approach to payment monitoring and measurement may be a growing challenge for many moving forward. And, of course, payment processors, acquiring banks, and third-party online marketplaces all remain indispensable payment partners for most merchants, collectively supporting their goals of reaching and delighting customers while ensuring smooth, profitable payment operations.

As merchants work to optimize payment offerings and operations, they are also striving to improve their strategies and tactics for mitigating payment fraud. This year's survey shows merchants contending with a continued increase in several forms of fraud, with rates of first-party misuse rising rapidly, in particular.

Despite significant internal obstacles, including lack of sufficient fraud management resources and perceived gaps in fraud tool functionalities, merchants are putting into place comprehensive strategies that leverage multiple techniques and solutions to try to rein in FPM and other prevalent fraud threats. These include tools and tactics tied to flagging & checking, verification and identification, & enhanced requirements, as well as utilizing card brands' updated compelling evidence rules to block or overturn FPM disputes.

There is never a "one size fits all" approach, as we see merchants adopting divergent strategies and goals for fraud prevention and management, with some prioritizing the customer experience as their guiding star, while others focus more on reducing fraud and chargebacks. These distinct priorities are driving different plans for tactical improvements and investments. Future waves of this study will shed more light on which strategic and tactical approaches work best, as merchants and payment and fraud enablers continue to partner and compete in today's complex eCommerce environment.

About The Authors

VISA Acceptance Solutions

Visa Acceptance Solutions helps businesses build the payments experiences of the future. We leverage the power 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 60+ 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

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 loss, 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 Merkle 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 indicate 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?
- For which reasons did your organization add new types of payment methods over the past 12 months?

Figure 5

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

Figure 6

- Please indicate how much you disagree or agree with each statement below.

Figure 7

- Which of the following types of payment methods does your organization currently accept?
- Among all the payment methods your organization currently accepts (shown below), which three methods have the highest fraud rates?

Figure 8

- 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 9

- 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 10

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

Figure 11

- 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 12

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

Figure 13

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

Figure 14

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

Figure 15

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

Figure 16

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

Figure 17

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

Figure 18

- Why does your organization utilize third-party marketplaces?

Figure 19

- 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 20

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

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

- Over the past 12 months, how much has each of these challenges negatively impacted your organization's ability to manage fraud?

Figure 24

- Over the past 12 months, how much has each of these challenges negatively impacted your organization's ability to manage fraud?

Figure 25

- 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 26

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

Figure 27

- Over the past 12 months, has your organization experienced an increase in first-party misuse?
- On average, how much does it cost your organization to resolve a (single) first-party misuse dispute?
- What percentage of all fraudulent disputes do you believe are first-party misuse?

Figure 28

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

Figure 29

- For what reasons do you believe your organization has seen an increase in first-party misuse disputes over the past year?
- Which of the following reasons do you believe causes first-party misuse to occur in your organization's eCommerce business?

Figure 30

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

Figure 31

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

Figure 32

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

Figure 33

- 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?

Figure 34

- Has your organization used card brands' updated compelling evidence rules to block or reverse first-party misuse disputes?
- Do you believe the updated compelling evidence rules will help your organization solve or reduce the problem of first-party misuse?
- How effective have card brands' updated compelling evidence rules been at successfully blocking illegitimate disputes caused by first-party misuse from being found in favor of the issuer?

Figure 35

- Which one of the following would you say is the most important to your organization when evaluating fraud management practices?

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

- 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 38

- 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 39

- 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 40

- 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 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?
- And which of these tools and techniques is your organization likely to consider adding in the next 12 months?