2023 Global Ecommerce Payments And Fraud Report

cybersource
A Visa Solution

MRC

VERIFI
A Visa Solution

Limitation of liability

The information, recommendations or “best practices” contained herein are provided “AS IS” and intended for informational purposes only and should not be relied upon for business, operational, marketing, financial, legal, technical, tax or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or “best practices” may vary based upon your specific business needs and program requirements.

By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations.

Cybersource is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Cybersource makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Cybersource shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Report contents

Overview

The Merchant Risk Council (MRC), Cybersource, and Verifi are pleased to present the results of the 2023 Global Ecommerce Payments & Fraud Survey, an educational report designed to convey transparent and unbiased research. This report is based on a global survey of more than 1,000 MRC and non-MRC merchants who were asked about their ecommerce payments and fraud management practices. The survey sample includes a diverse mix of small businesses (SMBs), mid-market and enterprise merchants, representing organizations based throughout the North American, European, Asia-Pacific (APAC) and Latin American (LATAM) regions. This research was conducted in November and December of 2022.

These survey results delve 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 why they are adopting these payment strategies and tactics in the current commercial environment. In addition, this research 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 thanks to all participating merchants for taking the time to complete the online survey, to Cybersource and Verifi for managing the research, and to B2B International for directing the program and analyzing the data.

Survey firmographics

The survey was fielded in November and December of 2022. A total of 1,072 merchants involved in ecommerce fraud and payment management (including 57 MRC member companies) participated in the research. The sample includes merchants based in four major geographic regions, with broad representation across size / revenue tiers, sales channels and categories. The breakdown of the merchant sample across key firmographics is shown in the figures below.

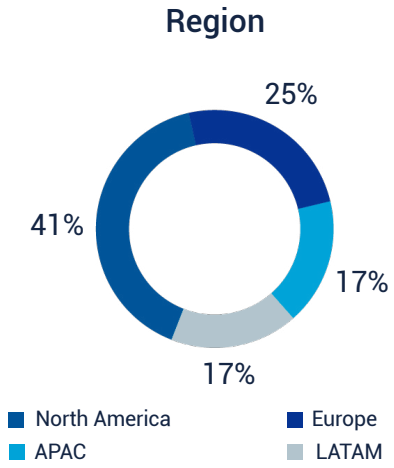


Figure 1

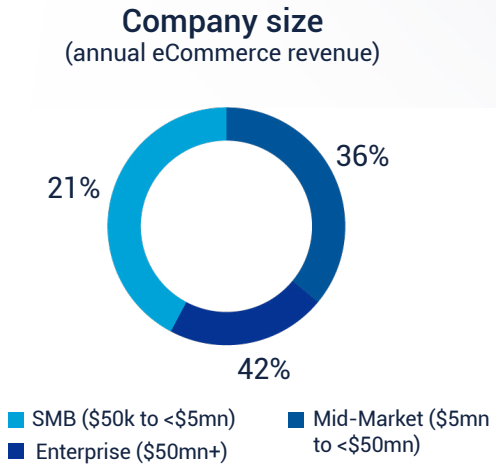


Figure 2

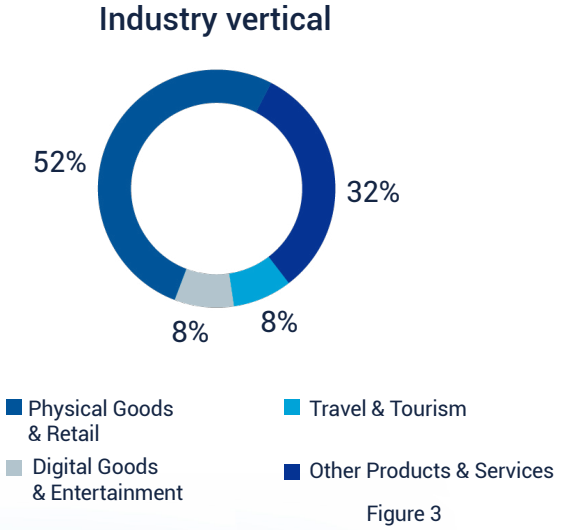


Figure 3

The global sample distribution by region and size segment was kept consistent, year to year. Some results may be driven by differences in the merchant populations surveyed in each region. Among the MRC members in the survey sample, two-thirds (67%) are based in North America, with the remainder largely based in Europe (29%). 9 out of 10 MRC merchants in the survey are large enterprises, generating over $50mn in annual ecommerce revenue.

Executive summary

The key findings from the 2023 Payments & Fraud survey are organized into five focus areas, or sections, in this report. Each section addresses a central question integral to understanding the state of ecommerce payments and fraud from the merchant perspective. The first two sections focus on insights pertaining to ecommerce payments, while the last three delve into topics related to ecommerce fraud.

These five focus areas, along with the key, high-level findings in each, are summarized below:

1. Payment Acceptance – How are merchants being paid?

- Bank transfers, digital wallets and cards continue to be the most widely accepted payment methods among ecommerce merchants. Roughly 90% of merchants take some measures to encourage customers to pay via certain, preferred methods, primarily to minimize fraud risks and maximize how quickly funds become available.
- Merchants are increasingly implementing **buy-now-pay-later (or "BNPL") payment methods**, with over one-third (36%) now offering customers this option. Acceptance of card payments also increased globally over the past year. BNPL payments, crypto payments and local digital payments (such as PIX and Alipay) stand out as the fastest-growing methods, with most who accept these having implemented them
- this year.
- Improving the customer experience is the top reason merchants add new payment methods, but reaching new customer segments or markets is an important driver, too. Similar motivations are driving merchants' increased usage of third-party marketplaces, with 8 in 10 transacting via the likes of Amazon, eBay and similar marketplace partners.
- Merchants continue to leverage multiple payment processors and acquiring banks to support omnichannel payments, although small merchants use significantly fewer of these partners than mid-market and enterprise businesses. Maximizing operational flexibility, geographic coverage, and payment authorizations top the list of merchant motivations for utilizing multiple acquirers.

2. Payment Management – How are merchants optimizing experiences & platforms?

- To keep up with fast-changing shopping habits and payment preferences, merchants continue to adopt and experiment with multiple new retail approaches and customer experiences. Over the past year, **BNPL and subscription / recurring purchases** saw the largest increases in usage, with over one-third of global merchants now offering these options, compared to roughly one-quarter in 2021.

- When it comes to new customer payment experiences, merchant usage of **chatbots and customer service AI programs**, as well as connected devices, increased substantially this year. In keeping with trends from previous years, enterprises and APAC-based merchants over-index significantly when it comes to embracing these new approaches and experiences, while adoption skews much lower among SMBs and MRC members.

- Merchants now employ an average of two to three different approaches or techniques designed to optimize payment authorization. In particular, usage of **machine learning** to fine-tune fraud management, as well as **intelligent payment routing**, have seen increased adoption over the past year, with around 4 in 10 now utilizing each of
- these approaches.

- As merchants utilize a larger array of payment methods, commerce partners and new retail approaches to serve customers, they are also **tracking a wider range** of payment **KPIs**. The share who track payment success rate, revenue and cost of payments all increased significantly over the past year, as did the percentage who keep a close eye on refund rates. On average, merchants now cite over four different payment KPIs as "extremely important" for their organization (up significantly versus last year).

3. Business Impacts Of Fraud – What are the effects of fraud on merchant businesses?

- Following a turbulent year in which fraud KPIs increased across the board, this year saw **encouraging improvement in several key fraud management metrics**, such as the share of ecommerce revenue lost to fraud, domestic order rejection and fraud rates, and the share of ecommerce orders that led to fraud-related chargebacks. Decreased fraud metrics were particularly evident in North America, where spending on fraud management rose markedly last year. This year, anti-fraud spending rose significantly in APAC and Latin America, as well as among small businesses, suggesting that these segments may hope to see improvement in their fraud metrics in the coming year.

- On the subject of manual order review, merchants' sentiments and future strategies have remained consistent over time, with around 6 in 10 seeking to reduce or eliminate this aspect of fraud management. Size of business is an important factor here, as SMBs are apt to try to reduce or eliminate manual review, while enterprises are likely to retain it.

    - This year, APAC and LATAM-based merchants also stood out as the only segments reporting significant increases in the percentage of manually screened orders that they subsequently decline.

- Roughly **85% of merchants have started implementing Strong Customer Authentication** (SCA) to comply with the EU's PSD2 regulations, but roughly half (49%) have yet to complete this process. Merchants in Europe & APAC, as well as large enterprises, are taking the lead in this area. As merchants have adjusted to PSD2/ SCA in recent years, there has been a sharp increase in the share who say it has added complexity to how they manage compliance (versus how they manage fraud and payments).

    - New questions added to this year's survey show **recurring transaction, secure corporate payment (SCP) and transaction risk analysis (TRA) are the top three SCA exemptions** likely to be used most widely by merchants, moving forward.

4. Fraud Attacks & Challenges – Where are merchants most vulnerable?

- Phishing / pharming / whaling attacks are still most prevalent. The incidence of this attack, as well as re-shipping attacks, increased markedly in the past year. MRC Members continue to cite a much larger and broader range of fraud attacks than non-members (reporting 6, on average, versus just 3 for non-members). First-party misuse, card testing & account takeover are particularly problematic for MRC merchants.

- **Over one-third of merchants experience first-party misuse or "friendly fraud," with enterprises in particular seeing a significant spike** in this activity. Roughly 9 in 10 submit compelling evidence to resolve friendly fraud disputes, and 7 in 10 are aware of card brands' recent updates to these policies. Those that are aware are generally quite optimistic these updates will help combat this thorny issue.

- Merchants cite **increasing challenges in managing ecommerce fraud** over the past few years. **Effectively using data and analytics to manage fraud has become a particularly pressing challenge and also a key focus area for improvement** this year. Merchants in APAC and Enterprises face a disproportionate number of fraud management challenges, in contrast to those in North America and SMBs. MRC members struggle more than non-members when it comes to fraud tool deficiencies & resource constraints.

5. Fraud Prevention – How are merchants addressing the issue of ecommerce fraud?

- Continuing a trend from last year's survey, merchants are more likely to prioritize preventing fraud and chargebacks, versus improving CX or minimizing costs. But merchants in Latin America are more evenly split on this question with equal shares prioritizing fraud prevention versus CX improvement.

- Merchants are **utilizing an increasing array of fraud detection tools** – five, on average – with over half using credit card and identity verification services. Enterprises use a significantly larger arsenal of fraud detection tools, while SMBs use fewer tools than average. MRC members use twice as many fraud detection tools as non-members, on average, which is likely linked to MRC merchants' much higher propensity to outsource fraud tools. But MRC members are far less likely than non-members to use two-factor phone authentication and credit history checks.

- The most widely used tools are generally rated the most effective, but **more merchants should consider using biometric indicators, individualized fraud scoring models**, & multi-merchant purchase velocity models, given these tools' low usage and high effectiveness.

Altogether, the insights and findings from this year's study indicate that merchants are striking an increasingly successful balance between leveraging technological tools and tactics and applying human knowledge and expertise to optimize payment & fraud management. This strategic challenge is evident in many of the trends and topics discussed throughout the report, making it one of the central themes emerging from our research this year.

1. Payment Acceptance and Partners

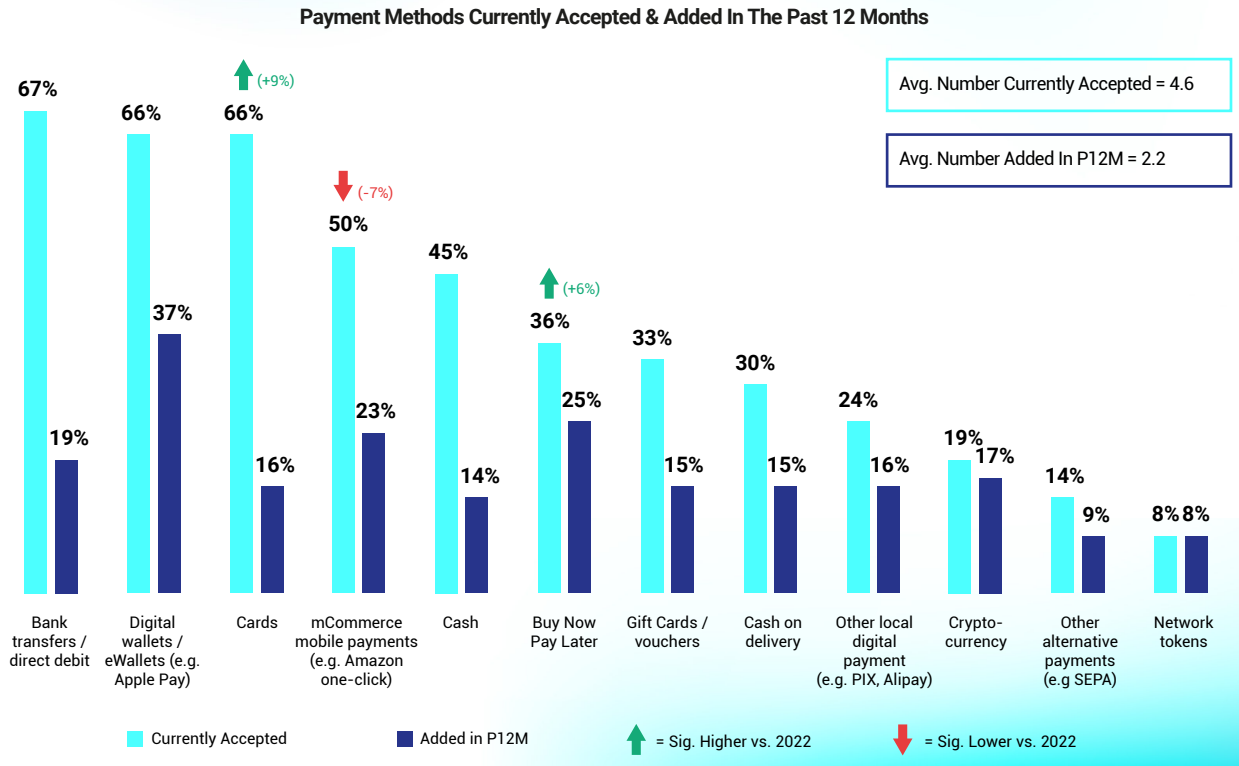
In the first two sections of this report, the focus is on ecommerce payments. Specifically, these sections examine how merchants are being paid by consumers and how they are managing and optimizing payment processes and operations.

This section delves into the question of how merchants are being paid – i.e., which payment methods they accept, how many processing and finance partners they use to support payment acceptance, and how their acceptance strategies and partnerships vary by region, size, and MRC membership status.

Direct Debit, Digital Payments And Cards Still Most Popular Payment Methods Accepted, With Buy Now Pay Later (BNPL) On The Rise

Globally, ecommerce merchants currently accept payments via four primary methods: digital wallets, direct debit transfers, traditional cards and mCommerce mobile apps (such as PayPal mobile or Amazon one-click). Cash is also accepted by nearly half of merchants, while gift cards and vouchers, third-party payments, and buy-now-pay-later (BNPL) payments are each accepted by around 3 in 10. Over the past 12 months, merchants have been most likely to add digital wallets, BNPL and mCommerce payments to their acceptance portfolio (see Figure 4). Localized digital payment methods, like PIX and Alipay, as well as cryptocurrency payments, also seem to be on the rise, as most merchants who accept these began doing so over the past 12 months.

Figure 4: Payment Methods Currently Accepted & Added In Past 12 Months (2023)



In addition to the year-over-year trends illustrated in Figure 4, our 2023 data also reveal notable differences in the types and numbers of payment methods accepted by merchants in different regions and size segments. Although cards, bank transfers / direct debit and digital wallet payments are the top three most widely accepted methods in all four regions, there are significant differences in acceptance of other forms of payment across different geographic markets. For instance, North American merchants are nearly twice as likely as those in Europe to accept cryptocurrency payments (23% vs. 13%). Latin American merchants skew higher than those elsewhere on acceptance of both card payments (at 79%) and local digital payments, like PIX (accepted by 46%). And merchants in APAC over-index on acceptance of digital wallet payments (76%), mCommerce mobile payments (59%), and BNPL (54%).

When it comes to the number or variety of different payment methods currently accepted, merchants in APAC and enterprise merchants tend to accept more payment methods than average, while merchants in North America and SMBs accept fewer than average (see Figure 5). Looking at the numbers of new acceptance methods added over the past year, it's clear that APAC merchants are embracing a broader approach than those in other regions – especially Europe – with the former group adding almost twice as many new payment methods as the latter, on average (see Figure 5).

Figure 5: Average Numbers Of Payment Methods Currently Accepted And Added In Past 12 Months (2023)

Average Numbers of Payment Methods Accepted & Added In Past 12 Months	Overall	By Region (2023)				By Ecommerce Revenue (2023)			By MRC Status (2023)	
		North America	Europe	APAC	LAT AM	SMB	Mid-Market	Enterprise	Non-Member	MRC Member
Base	1,072	440	269	180	177	391	226	455	1,015	57
Average No. Of Payment Methods Accepted	4.6	4.3	4.4	5.3	4.7	4.2	4.5	5.0	4.6	5.1
Average No. Added In Past 12 Months	2.2	2.1	1.7	3.2	2.0	1.7	2.2	2.5	2.2	0.9

= Sig. Higher = Sig. Lower

Also, MRC merchants take a notably different approach to payment acceptance than non-members. MRC merchants are significantly more likely to accept cards, digital wallets, gift cards or vouchers and other alternative payments, such as SEPA and Giropay (see Figure 6). MRC members also lead adoption of BNPL, with 47% accepting this method, compared to 35% among non-members. But non-members seem to be catching on quickly with BNPL, as this year's survey shows a significant rise in the share who accept it, compared to last year.

Figure 6: Differences In Payment Acceptance Among MRC Members vs. Non-Members

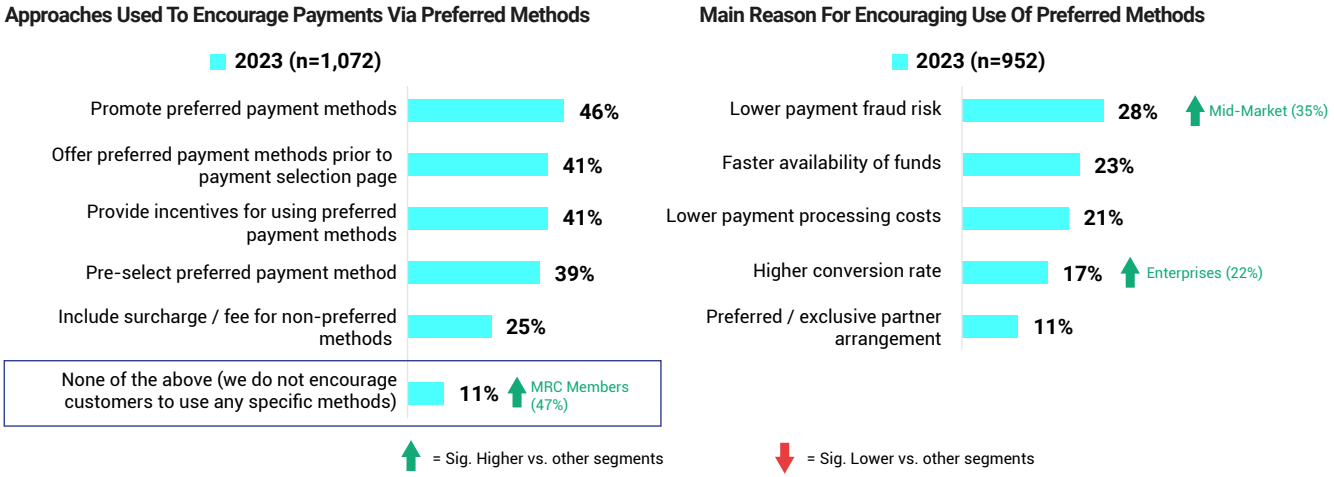
Share of Merchants Currently Accepting Each Payment Method	By MRC Status (2023)		
	Overall	Non-Member	MRC Member
Base	1,072	1,015	57
Bank transfers / direct debit	67%	68%	49%
Digital wallets / eWallets	66%	66%	82%
Cards	66%	64%	96%
mCommerce mobile payments	50%	51%	32%
Cash	45%	46%	30%
Buy Now Pay Later	36%	35%	47%
Gift Cards / vouchers	33%	32%	56%
Cash on delivery	30%	31%	11%
Other local digital payment method	24%	24%	37%
Cryptocurrency	19%	19%	11%
Other alternative payments (SEPA, Giropay, etc.)	13%	12%	49%
Network Tokens	8%	8%	7%

= Sig. Higher = Sig. Lower

Another aspect of payment acceptance in which MRC merchants diverge from non-members is when it comes to encouraging payments via certain, preferred methods. While 9 out of 10 merchants globally encourage payments via preferred methods, the same is true of only around half of MRC members (see Figure 7). The vast majority of merchants who do encourage payments via preferred methods mainly do so to lower fraud risk, expedite availability of funds, and lower payment processing costs.

Typical approaches used by merchants to encourage such payments include promoting and incentivizing the use of preferred methods (for instance, through discounts or reward programs), offering preferred methods prior to the main payment selection page, and pre-selecting preferred methods as default payment options for customers. (see Figure 7).

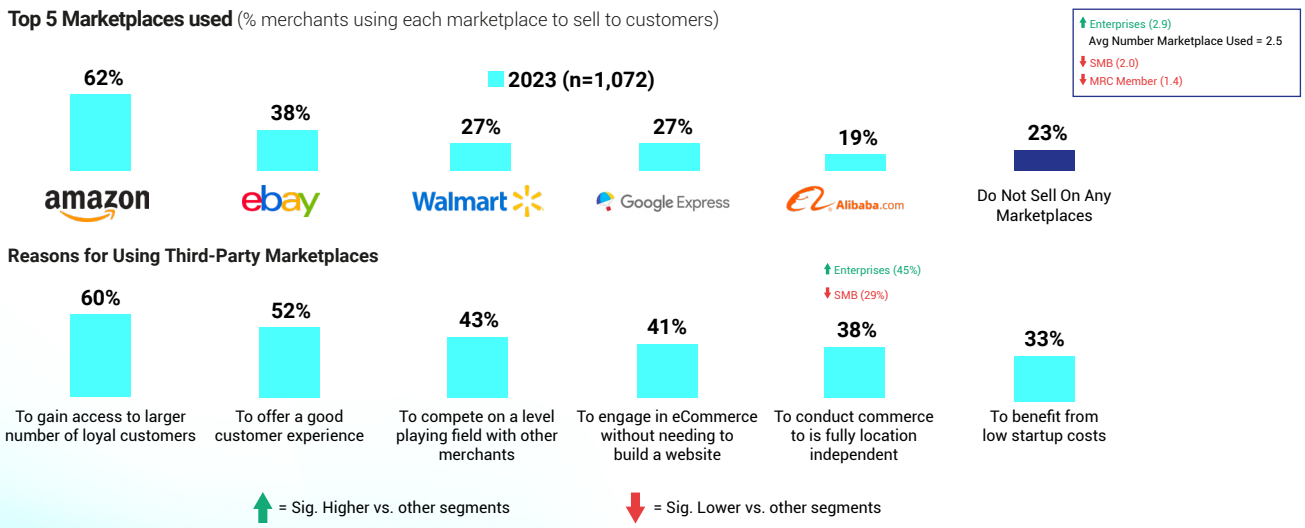
Figure 7: Approaches And Reasons For Encouraging Ecommerce Payments Via Preferred Methods



Third-Party Marketplaces Remain Key Partners, Especially For Large & Midsize Merchants

Over three-quarters (77%) of merchants sell through third-party marketplaces, like Amazon and eBay and Alibaba (see Figure 8). Midsize and enterprise merchants over-index on using marketplaces to support online business, in contrast to SMBs. Non-MRC members are also far more likely to sell through marketplaces than MRC members. Gaining access to the large numbers of loyal customers that use these marketplaces is the primary reason merchants utilize them, although other motivations are also at play, like offering good customer experiences and being able to compete with other merchants on a level (and global) playing field (see Figure 8).

Figure 8: Usage Of Top Third-Party Marketplaces And Reasons For Using Them



Payment Acceptance Supported By Multiple Processor and Acquirer Partners

While online marketplaces may occupy the gray area between cooperation and competition with ecommerce merchants, there are other third-party partners – specifically, payment processors and acquiring banks – that are far more essential to supporting payment acceptance offerings.

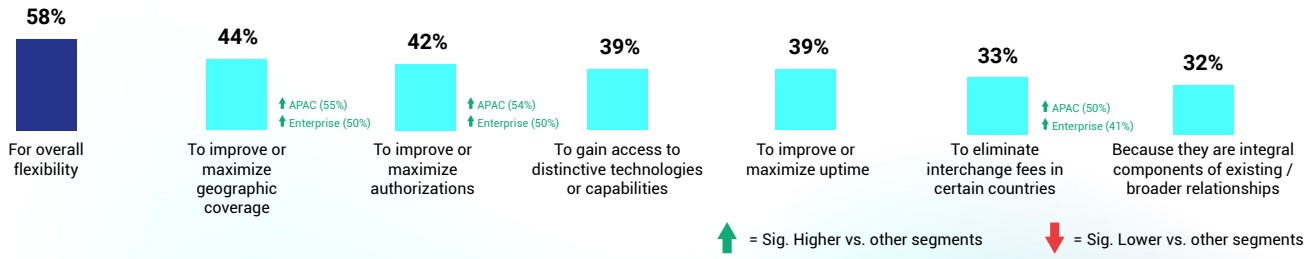
On average, merchants rely on roughly four payment processor or gateway connections and three acquiring banks to support omnichannel payments, although these figures skew a bit higher for APAC and LATAM-based merchants and lower for those in North America. Enterprise merchants also tend to use more of these partners than SMBs (see Figure 9).

Maximizing flexibility, geographic coverage, and payment authorizations represent the main reasons why merchants utilize multiple acquirers. APAC-based merchants and enterprises tend to cite additional reasons, as well – for instance, eliminating interchange fees in certain countries. This partly explains why these segments tend to use more of these partners than merchants based in other regions and size segments.

Figure 9: Usage Of Payment Processors & Acquiring Banks To Support Payment Acceptance

Number Of Payment Partners Used (Trimmed averages shown for both)	Overall 2022	Overall 2023	By Region (2023) North America	Europe	APAC	LAT AM	By Ecommerce Revenue (2023) SMB	Mid-Market	Enterprise	By MRC Status (2023) Non-Member	MRC Member
Number Of Payment Gateway / Processor Connections Currently Supported	4.1	3.9	3.5	3.8	4.5	4.7	3.2	4.2	4.3	4.0	3.3
Number Of Merchant Acquiring Banks Currently Used	3.2	3.4	2.9	3.2	4.1	3.9	2.7	3.4	3.9	3.4	2.9

Reasons For Using Multiple Acquiring Banks (among n=806 merchants using 2 or more acquiring banks)



2. Payment Management

In this section, we examine what merchants are doing to improve and innovate customer payment experiences and to optimize internal payment management processes and operations. Notable payment management trends uncovered by our survey this year include an uptick in merchants offering Buy Now Pay Later (BNPL) and subscription payment options, more integration of chatbots, AI and machine learning to support customer-facing and internal payment operations, and a heightened focus on tracking several important payment management metrics, or KPIs.

More Merchants Implementing Novel Retail Approaches And Customer Experiences

This year's results show increasing usage of several novel retail approaches and customer experiences, suggesting that more merchants may be moving past the experimentation stage with these approaches and aiming for full adoption and integration over the coming years. Overall, merchants are using an average of 3.6 new retail approaches this year (up from 3.4 last year) and an average of 2.8 new customer experiences (up from 2.6 last year). Detailed, year-over-year data for both of these questions is displayed in Figure 10, below.

Figure 10: Usage Of New Retail Approaches & Customer Experiences – 2023 vs. 2022

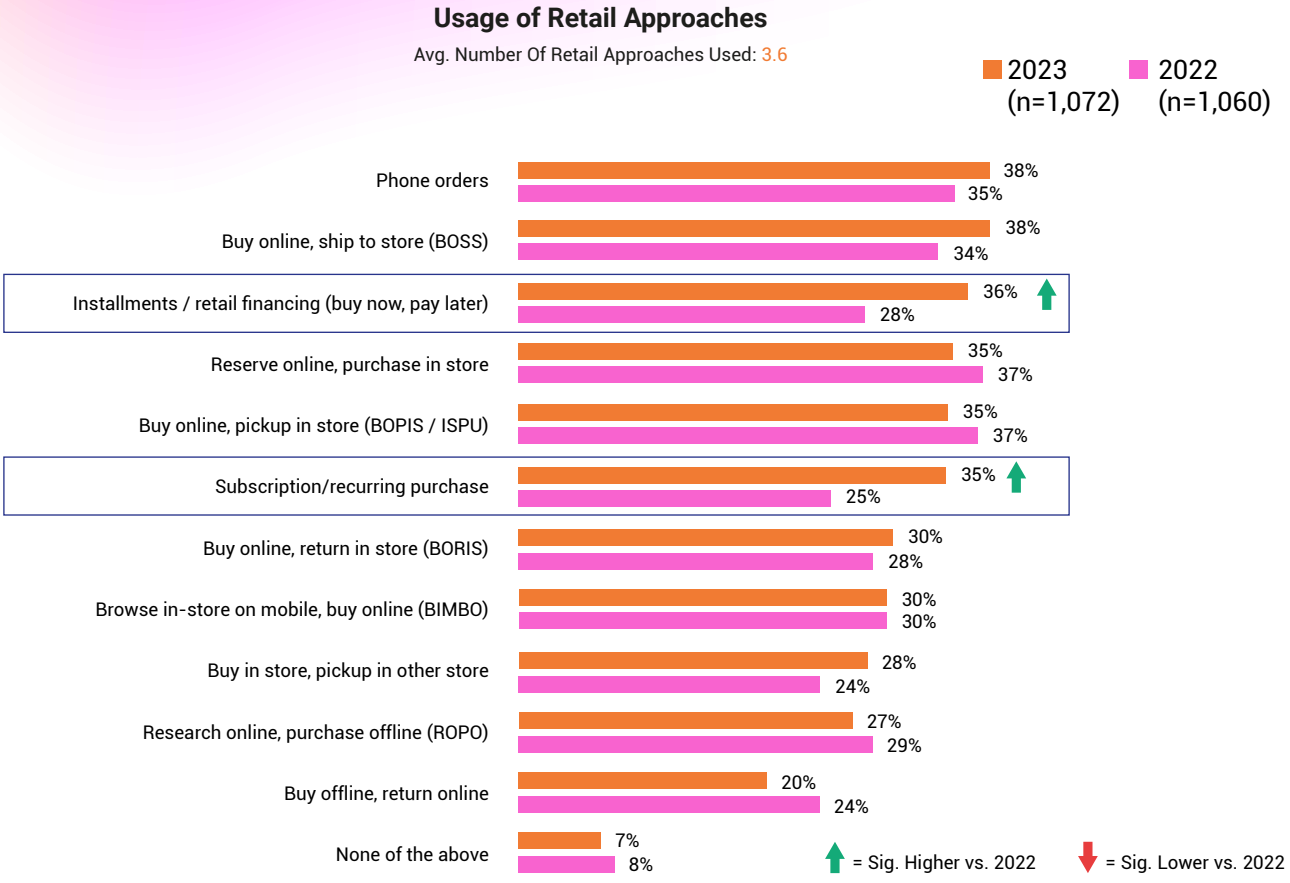
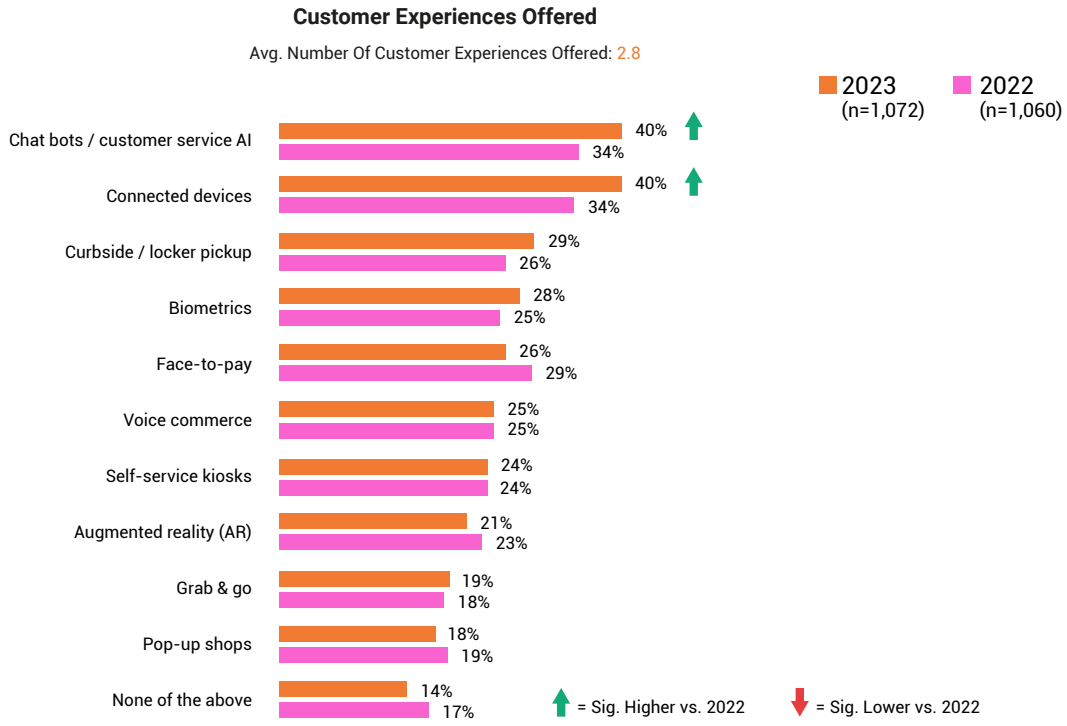


Figure 10: Usage Of New Retail Approaches & Customer Experiences – 2023 vs. 2022



In terms of new retail approaches, there was around a 10% uptick in the share of merchants offering Buy Now, Pay Later options (also known as installments or retail financing), as well as a similar increase in the share offering subscription or recurring purchase programs. Over one-third of merchants globally are leveraging these two approaches. As with many other aspects of payment and fraud management, midsize and enterprise merchants are leading the way in adopting and integrating these into their selling strategies.

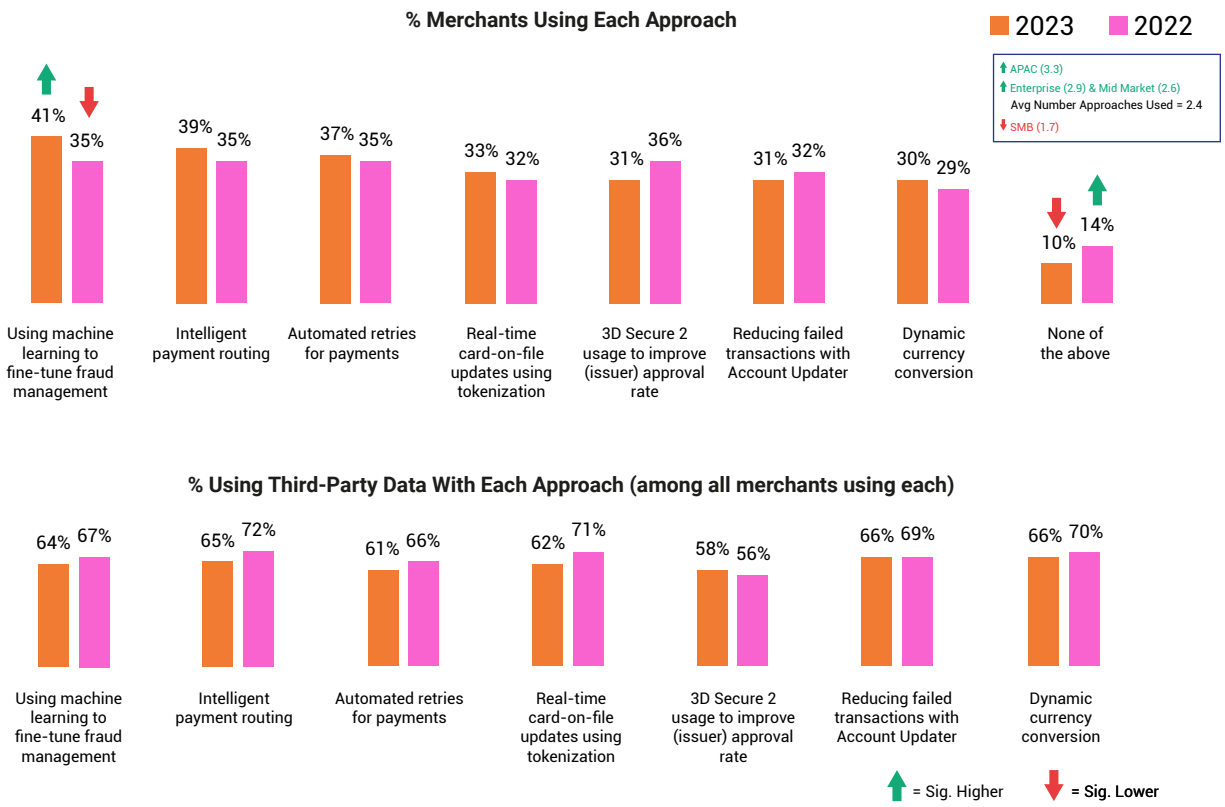
When it comes to new customer experiences, 40% of merchants are now leveraging chatbots or customer service AI programs, as well as those utilizing connected devices to provide customers with more seamless and streamlined omnichannel experiences. Examples of chatbot and AI programs introduced by U.S. merchants include Domino's Pizza's chatbot called Dom, which makes it easy for customers to place orders on the go via the Facebook Messenger app and Sephora's Virtual Artist – a mobile application that allows customers to "try on makeup instantly" using only a smartphone. Connected devices also enable more seamless payment transactions (e.g., via tap-to-pay solutions embedded on smartphones), as well as physically touchless transactions – an increasingly critical benefit, following the global COVID-19 pandemic. With such a sizable share of merchants leveraging these two tactics, their global usage rate now well exceeds all other new experiences tested in our survey – e.g., curbside pickup, biometric payments and pop-up shops.

Increasing Usage Of Machine Intelligence To Optimize Internal Payment Processes

Merchants tend to employ two to three different approaches or techniques designed to optimize payment authorization, internally. In particular, usage of machine learning to fine-tune fraud management, as well as intelligent payment routing, have seen increased adoption over the past year, with around 4 in 10 now utilizing each of these approaches (see Figure 11). Merchants in Asia, as well as enterprise and mid-market merchants, are using more of these approaches than average, in contrast to small businesses. While fraud management has historically been seen as a separate function to payment processing, sophisticated fraud management is also seen today as a means of optimizing payment authorization through its emphasis on lowering of false positives and even influencing issuer acceptance by achieving lower merchant fraud rates.

Also shown in Figure 11 is the share of merchants saying they use third-party data to support each of these authorization-boosting approaches. On this question, we saw a small but consistent trend of retrenchment among merchants, with slightly fewer utilizing third-party data this year, compared to last year, to support authorization-related approaches.

Figure 11: Usage Of Payment Authorization Approaches & Percent Using Third-Party Data With Each – 2023 vs. 2022

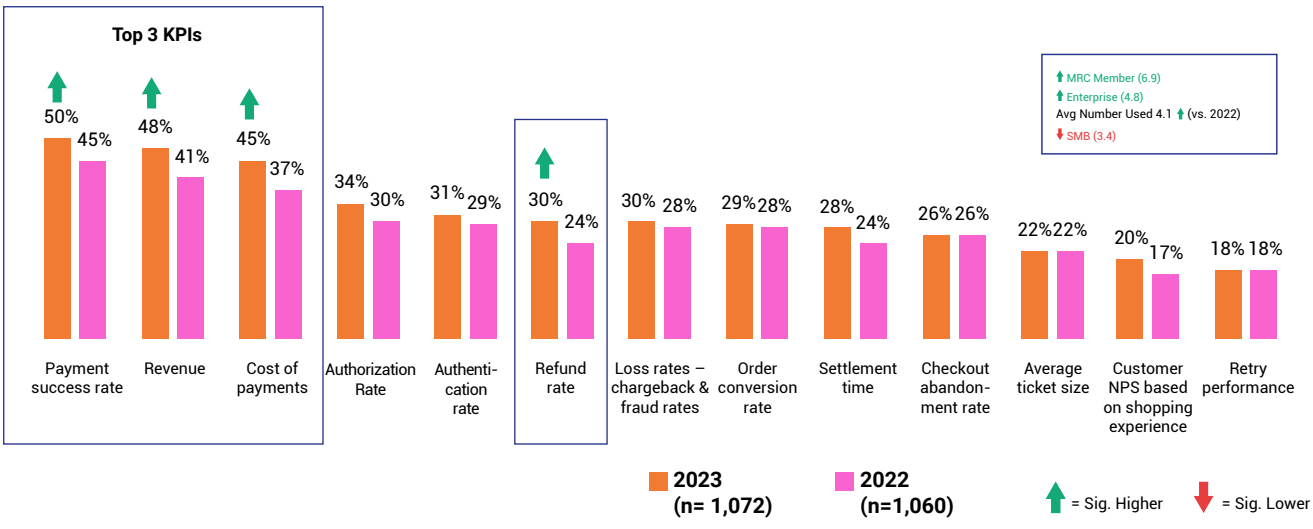


Merchants Keeping A Closer Eye On Several Payment Metrics, Including Refund Rate

As merchants deploy new customer-facing and internal payment management approaches, they are also keeping a closer eye on a range of important metrics, or KPIs. On average, merchants now rate 4.1 payment KPIs as extremely important to their organization – up significantly from an average of 3.7 last year. The shares of merchants who monitor success rate, revenue and cost of payments all rose significantly since 2022, as did the share who track refund rates (see Figure 12).

Here again, our data show larger merchants taking more advanced and comprehensive approaches to payment management, with enterprises tracking five of these payment KPIs, on average, while SMBs tend to keep tabs on just three or four.

Figure 12: Payment Management KPIs – 2023 vs. 2022



Additionally, our data indicates that MRC merchants are especially intent on measuring and monitoring their payment metrics; they track an average of seven different KPIs tested in our survey – nearly twice as many as the average non-MRC merchant.

3. Business Impacts of Fraud

The last three sections of this report shift our focus from ecommerce payments to ecommerce fraud. In this section, we delve into data around the costs of managing fraud and examine how fraud KPIs have changed over the past year to understand, at a high level, whether merchants have been more or less successful in applying financial resources to thwart and mitigate the negative impacts of ecommerce fraud on their businesses. We also revisit the topics of manual order review and the implementation of Strong Customer Authentication (SCA) to understand how merchants are thinking about and acting on these issues, now and in the near future.

Fraud-Related KPIs Exhibit Encouraging Declines, Especially On Domestic Orders

Following a turbulent year in which fraud KPIs increased across the board, merchants reported some improvement in fraud-related KPIs over the past 12 months, especially in relation to domestic business. As evidenced by the data table in Figure 13, the percentage of ecommerce revenue lost to fraud globally, order rejection and fraud rates on domestic orders, and the share of ecommerce orders that led to fraud-related chargebacks all declined significantly versus the prior year.

Decreased negative fraud metrics were particularly dramatic in North America, where we saw spending on fraud management increase markedly last year. APAC-based merchants, midsize and enterprise merchants, and both MRC members and non-members also cited statistically significant declines in various key metrics, in line with the general, positive trend this year of declines across the board.

Figure 13: Fraud Management KPIs – 2023 vs. 2022

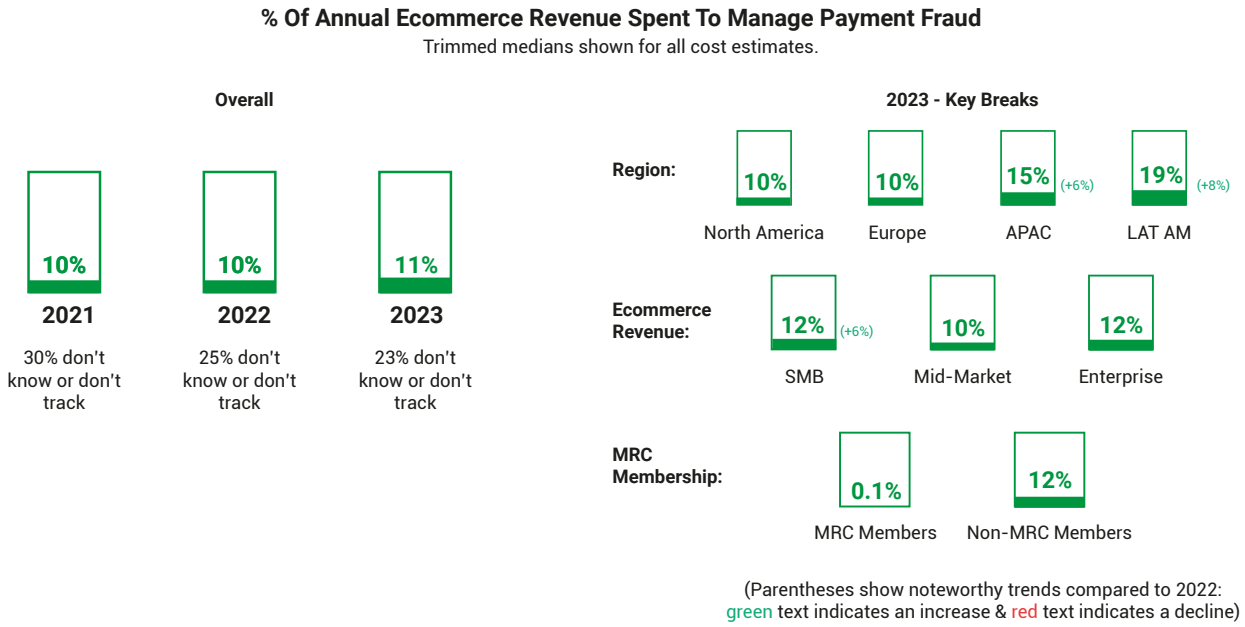
Fraud Management KPIs (2022 figures in blue) Trimmed averages shown for all KPIs			By Region				By Revenue			By MRC Status	
	2022	2023	North America	Europe	APAC	LAT AM	SMB	Mid-Market	Enterprise	Non-Member	MRC Member
% of eCommerce revenue lost to payment fraud globally	3.6	2.9 ↓	2.4 ↓ 3.6	3.1 3.0	2.9 ↓ 4.3	4.6 4.2	2.7 2.9	3.3 ↓ 4.1	2.8 ↓ 3.7	3.2 3.7	0.3 ↓ 0.7
% of eCommerce revenue lost to payment fraud from domestic orders	3.4	3.0	2.4 ↓ 3.6	3.3 2.8	3.0 3.3	3.9 3.6	2.8 3.0	3.2 3.8	2.9 3.4	3.2 3.5	0.2 0.4
Order rejection rate for domestic orders	3.4	2.7 ↓	2.4 ↓ 3.6	2.7 2.8	3.2 2.9	3.3 4.4	2.1 2.8	2.9 ↓ 3.9	3.1 3.6	2.8 ↓ 3.4	1.8 2.1
Order rejection rate for international orders	6.0	5.3	4.4 ↓ 6.3	5.3 5.1	6.0 5.3	6.1 7.0	4.1 5.3	5.3 6.7	5.8 6.0	5.5 6.1	2.9 3.0
% of domestic eCommerce orders that turned out to be fraudulent	3.1	2.6 ↓	2.2 ↓ 3.2	2.9 2.7	2.5 2.9	3.5 3.4	2.3 2.6	3.1 3.7	2.6 3.1	2.8 3.2	0.3 0.6
% of international eCommerce orders that turned out to be fraudulent	3.4	3.0	2.5 ↓ 3.3	3.2 3.0	2.6 3.7	3.8 4.0	2.7 3.0	3.1 3.8	3.0 3.3	3.2 3.5	0.3 0.7
% of eCommerce orders that led to chargebacks (due to fraud)	3.1	2.6 ↓	2.2 ↓ 3.4	2.7 2.3	2.8 2.9	3.7 3.8	2.4 2.6	2.8 ↓ 3.7	2.8 3.3	2.8 ↓ 3.2	0.2 0.2

↓ = Sig. Decrease In Fraud KPI ↑ = Sig. Increase In Fraud KPI

Spending On Fraud Management Remains Relatively Consistent

Globally, merchants continue to spend about one-tenth of their annual ecommerce revenue to manage payment fraud – a figure that has stayed quite consistent for three consecutive years in our study. We have also seen a notable decline in the share of merchants who tell us that they "don't know" or "don't track" this metric – from 30% in our 2021 study to 23% this year – suggesting that merchants are keeping a closer eye on fraud management spending as time goes on (see Figure 14).

Figure 14: Spending To Manage Payment Fraud (Relative To Annual Ecommerce Revenue)



From a geographic perspective, merchants in North America and Europe are spending about the same this year as they did last year to manage payment fraud. By contrast, those in APAC and Latin America have markedly increased spending over the past year – by 6% for the former and 8% for the latter. In fact, merchants in LAT AM are now spending nearly twice as much as the global average to manage payment fraud (19% versus 11%).

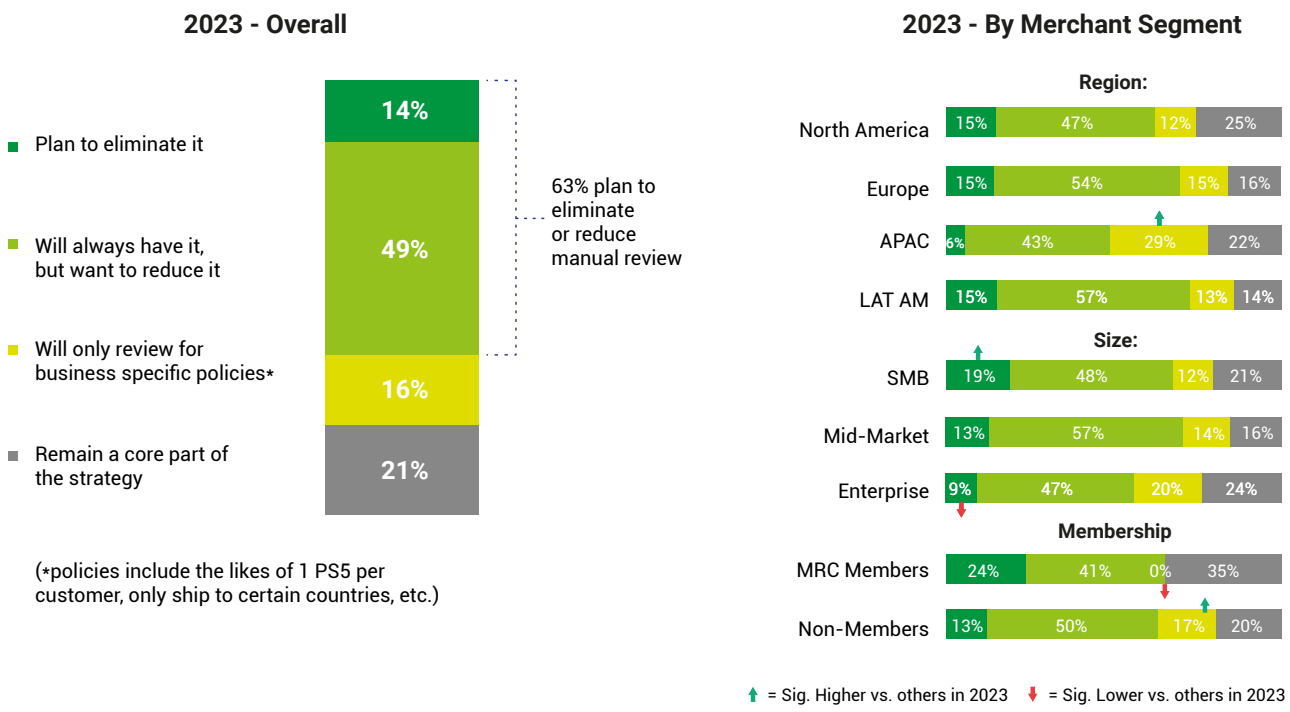
Also noteworthy is the increased spending on fraud management among the smallest merchants in our study – SMBs that generate between $50,000 and $5 million in annual ecommerce sales. These merchants essentially doubled their estimated fraud management spending over the past year, from 6% to 12% of ecommerce revenue.

In last year's study, we saw merchants in North America increase their fraud management spending dramatically, and that was followed by significant declines in the fraud KPIs they reported to us this year (see Figure 13). If a similar pattern holds true, merchants in APAC and Latin America, as well as SMBs, should see positive effects from their increased spending in the form of improved fraud metrics over the year to come.

Manual Order Review Still Important In Fraud Prevention, But Most Want To Reduce It

As illustrated by the data in Figure 15, over 60% of merchants plan to eliminate or reduce the amount of manual order review they engage in as part of their fraud prevention efforts – a proportion that has remained consistent over our past three years of research. Merchants based in APAC are significantly less likely to take this view, however, and instead far more likely than those in other regions to say they will only conduct manual reviews for business-specific policies (e.g., when shipping to certain countries or handling orders for certain products).

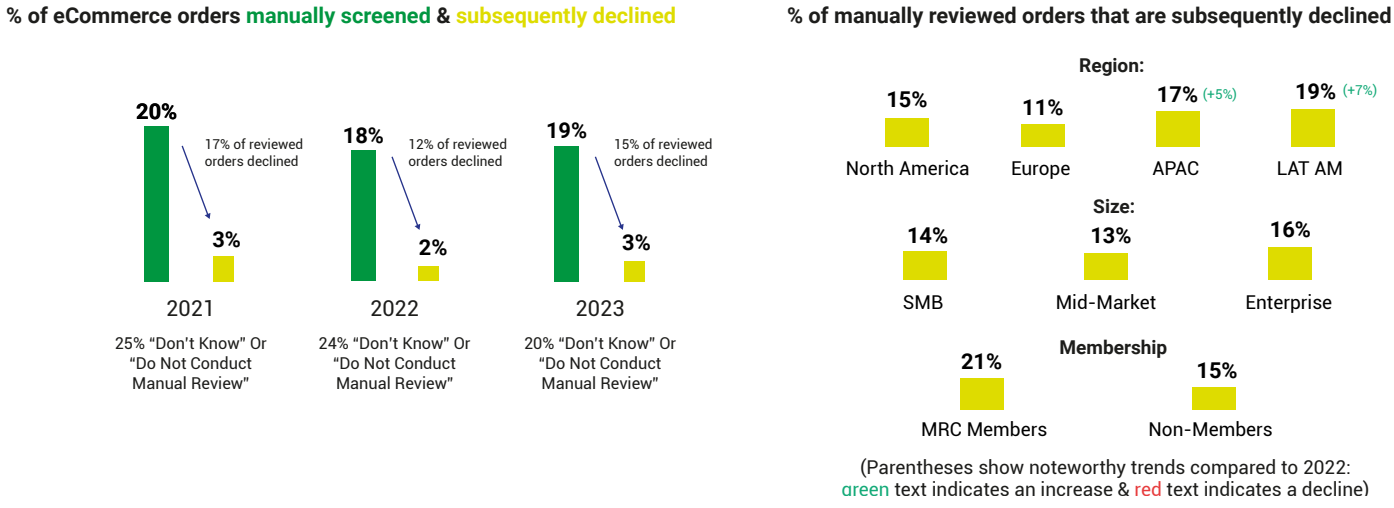
Figure 15: Role Of Manual Review In Merchants' Fraud Prevention Strategies (2023)



Size of business also matters when it comes to future plans for manual review, as SMBs are more likely to say they plan to eliminate this process entirely, while enterprises are significantly less likely to attempt this approach.

Just as merchants' plans and expectations concerning manual review have remained relatively consistent over the past few years, so too have their actions, in terms of carrying manual reviews out, in practice. After registering a slight decline last year in the share of ecommerce orders manually screened and subsequently declined, these figures ticked upward slightly in this year's survey. Globally, merchants now screen an average of 19% of all ecommerce orders manually, 15% of which they end up declining (see Figure 16). In other words, merchants manually screen about one out of five online orders they receive, and out of all of the orders that they review, they end up declining around one out of seven.

Figure 16: Screening & Declining Ecommerce Orders Using Manual Review



Merchants in the Asia-Pacific and Latin America regions significantly increased the share of manually screened orders that they ended up declining, compared to the previous year, which may partly explain why spending on fraud management also rose significantly for merchants in these two regions (see Figure 14).

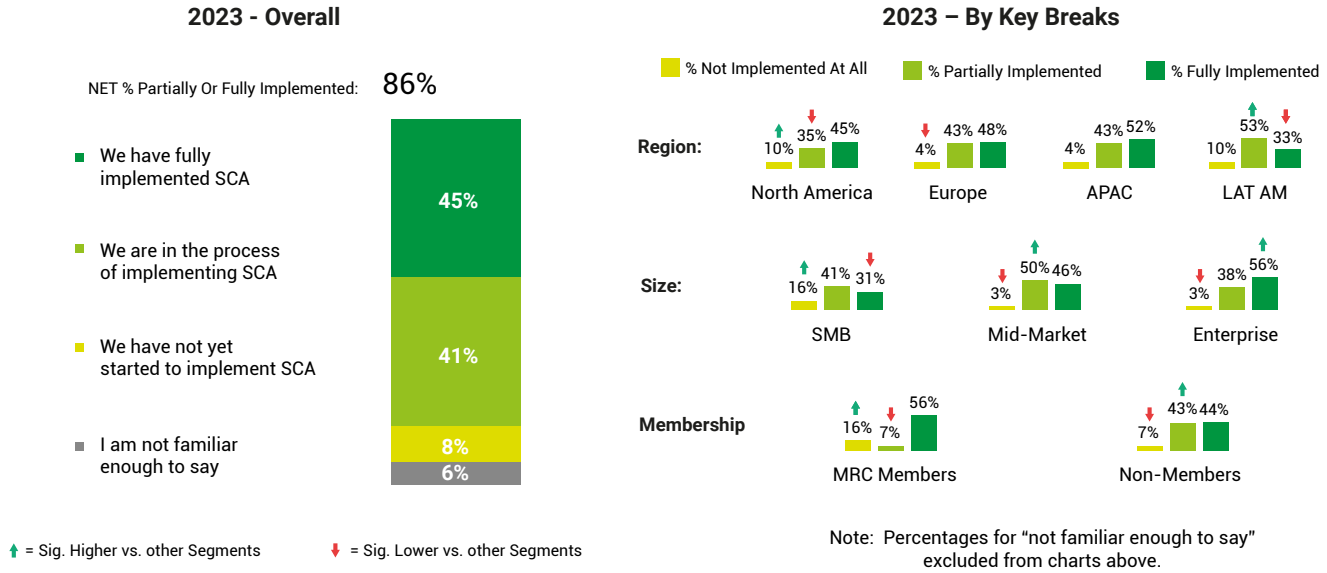
Notably, MRC members approach manual review quite differently than non-members. As shown in Figure 15, MRC members are far less likely to conduct reviews based on business-specific policies and instead more likely to say they either plan to eliminate reviews entirely or to retain manual reviews indefinitely as a core part of their strategy. In addition, MRC members decline a greater percentage of their manually screened orders than non-members – 21% for the former, compared to 15% for the latter (see Figure 16). These data could indicate that either MRC merchants are faced with a higher share of fraudulent orders than non-members or that they have different tools, tactics or techniques in place for conducting manual review, which result in them declining a somewhat higher percentage of the orders they screen manually.

The differences in manual review metrics between MRC members and non-members, as well as large enterprise merchants and smaller merchants more generally, may indicate that the latter segments are leading the way in figuring out how, where and when to best apply technological solutions versus human expertise and labor to tackle the problem of manual review.

Implementation Of SCA Is Well Underway, But Most Have Yet To Complete The Process

Progress is well underway, in terms of merchants implementing Strong Customer Authentication (or SCA), which is required to comply with the EU's updated Payment Services Directive, or PSD2. But while 86% of merchants have started to implement SCA, only 45% say they have done so fully – in other words, most still have work to do to complete the implementation process (see left side of Figure 17).

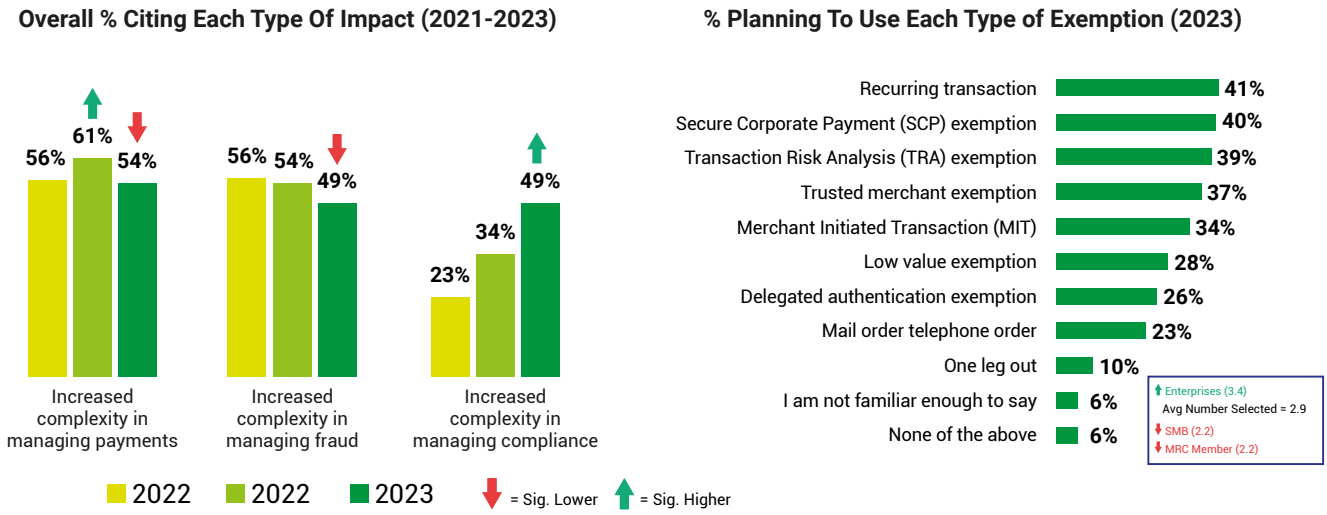
Figure 17: Merchant Implementation Of Strong Customer Authentication (SCA)



As shown in the data on the right-hand side of Figure 17, Europe- and APAC-based merchants are leading the charge to implement SCA from a geographic perspective, while enterprises and are farthest along among business in different size segments.
The majority of MRC members surveyed have fully implemented SCA, but there also seems to be a segment of MRC merchants who are lagging behind, as 16% have not yet begun the process at all, compared to only 7% among non-MRC members.

For the past three years, we have asked merchants what impacts SCA implementation is having or will have on their business. Looking at their responses to this question over time (as shown in the left side of Figure 18) reveals an interesting trend: As time has passed and merchants have gotten further into the implementation process, the percentages who say SCA implementation has increased the complexity of managing payments and managing fraud have significantly declined. Conversely, the share of merchants who say this process has increased the complexity of how they manage compliance has sharply risen. Currently, merchants seem to be evenly split on all three of these dimensions, with roughly half saying implementation has increased complexity in each of the three areas.

Figure 18: Business Impacts Of SCA Implementation (2021-2023) & Planned Usage Of SCA Exemptions (2023)



This year, we added one additional question on the subject of SCA to understand what types of SCA exemptions merchants plan to use in the future. This data is shown on the right side of Figure 18. Overall, merchants cited an average of around three SCA exemptions they plan to use, with recurring transactions, Secure Corporate Payment, and Transaction Risk Analysis exemptions being selected by around 4 in 10 merchants, respectively. Trusted merchant and Merchant Initiated Transaction exemptions were also popular, with over one-third planning to use each of those, as well.

Not surprisingly, enterprise merchants over-index on the number of exemptions they will likely make use of, while the opposite is true for small businesses. MRC Members also under-index when it how many exemptions they plan to use, averaging only 2.2, versus 2.9 among non-members (see right side of Figure 18). In fact, MRC members are more likely than most to say they have no plans to use any SCA exemptions, given that 14% of them selected this response, in contrast to just 6% among non-members.

4. Fraud Attacks & Challenges

This section starts by examining the most prevalent types of fraud ecommerce merchants experience and how their incidence fluctuates over time and across different segments of the merchant population. First-party misuse, or "friendly fraud," is one particular focus in this area of insights. Next, we move on to review merchants' top fraud-related challenges, as well as the most important areas for improvement that merchants will be prioritizing in their fraud-prevention efforts over the next 12 months.

Top Fraud Attacks Remain The Same Overall, With Friendly Fraud Rising From #4 To #2

Globally, the four most widespread forms of fraud stayed consistent for the third consecutive year of our study. These top four fraud attacks, from most to least prevalent, are phishing / pharming / whaling, first-party misuse (also known as "friendly fraud"), card testing and identity theft (see Figure 19).. Consistent with prior years of our study, merchants were impacted by three different types of fraud, on average, with SMBs under-indexing around two and large enterprises more apt to grapple with four or more.

Figure 19: Types Of Fraud Experienced By Merchants – Past 3 Year Rankings & Global Incidence (2023)

	2021 Rank	2022 Rank	2023 Rank	Global % Experiencing (2023)
Phishing / pharming / whaling	3	1	1	**43%** ↑
First-Party Misuse (i.e., friendly / chargeback fraud)	1	4	2 ●	34%
Card testing	2	2	3 ●	33%
Identity theft	4	3	4 ●	33%
Coupon / discount / refund abuse	5	7	5 ●	30%
Account takeover	7	5	6 ●	27%
Loyalty fraud	6	6	7 ●	22%
Affiliate fraud	8	8	8	22%
Re-shipping	12	11	9 ●	**20%** ↑
Botnets	10	9	10 ●	19%
Triangulation schemes	9	10	11 ●	17%
Money laundering	11	12	12	15%
AVG. # of attacks experienced	**3**	**3**	**3**	**3**

● Increased Ranking ● Decreased Ranking ↑ = Sig. Higher vs. 2022

Looking at how incidence of fraud attacks has shifted since our 2022 report, phishing / pharming / whaling attacks showed a significant increase in global incidence, with 43% of merchants experiencing this type of fraud, up from 35% last year (see Figure 19). The rate of first-party misuse also ticked upward, affecting just over one-third of merchants globally, which put its incidence just above that of card testing and identity theft. Occurrences of coupon / discount / refund abuse increased from 25% to 30%, vaulting that type of fraud back up to #5 overall, from #7 last year. And further down the list, the share of merchants impacted by re-shipping schemes also rose by 5%, from 15% to 20% in this year's study. This increase ranks re-shipping in the top 10 most common types of fraud for the first time the past three years.

MRC Members Continue To Combat A Larger Number And Variety Of Fraud Attacks

This year's survey once again highlighted a huge difference between MRC members and non-members, in terms of the number and variety of fraud attacks experienced by each group. As illustrated by the data in Figure 20, MRC merchants continue to register and report more than twice as many forms of fraud as non-members – six, on average, compared to three for non-members. In particular, MRC members are far more likely to experience friendly fraud (91%), card testing (85%), coupon / discount / refund abuse (57%), and account takeover (83%). In addition, the majority of MRC members must also grapple with less-common forms of fraud – e.g., botnets and triangulation schemes (57%, respectively).

While this trend of MRC merchants reporting more attacks than non-members has been clear and consistent over the past few years of our survey, it remains an open question whether this is due to MRC members actually experiencing a larger number and range of attacks or to MRC members having more fraud detection tools in place, which allows them to identify and register a larger share of the attacks that impact their businesses (or some combination of the two).

Figure 20: Fraud Attack Incidence Rates By MRC Membership Status (2023)

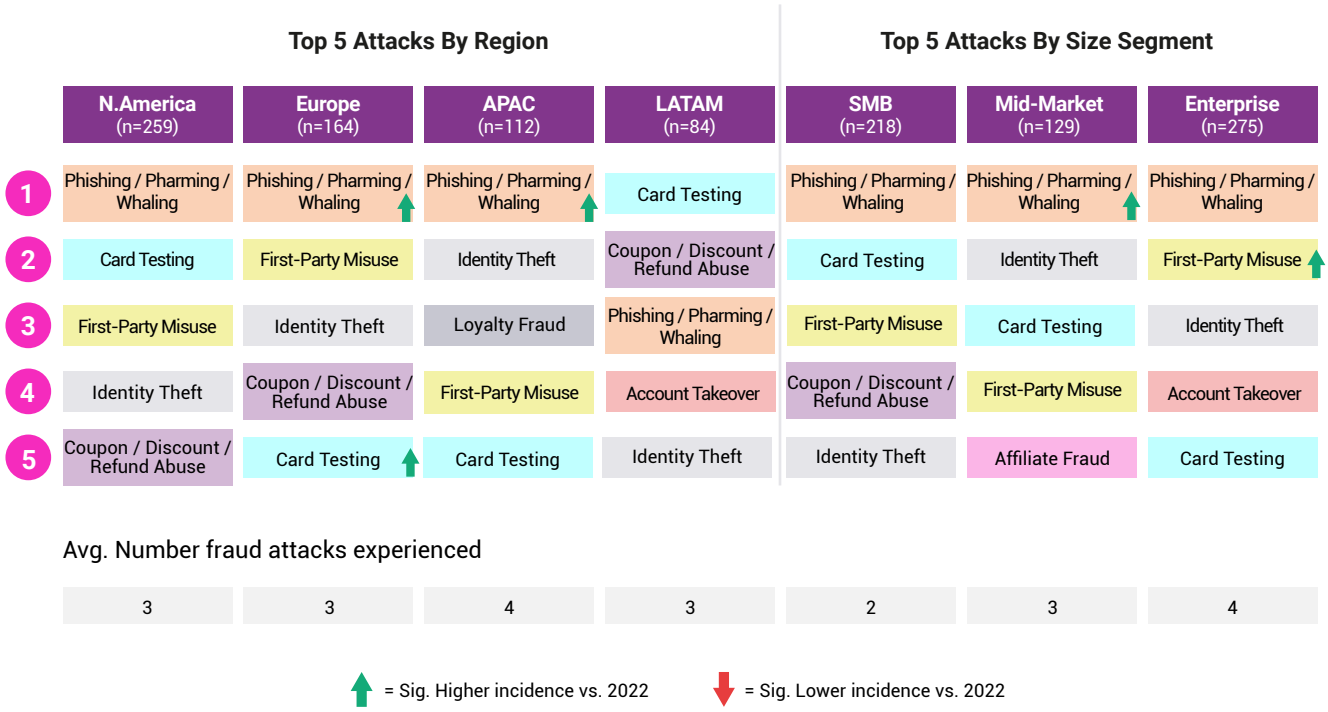
	% Non-Members Experiencing (N=576)	% MRC Members Experiencing (N=46)
Phishing / pharming / whaling	42%	54%
First-Party Misuse (i.e., friendly / chargeback fraud)	29%	**91%** ↑
Card testing	29%	**85%** ↑
Identity theft	31%	**50%** ↑
Coupon / discount / refund abuse	27%	**57%** ↑
Account takeover	23%	**83%** ↑
Loyalty fraud	22%	26%
Affiliate fraud	23%	20%
Re-shipping	18%	**48%** ↑
Botnets	16%	**57%** ↑
Triangulation schemes	14%	**57%** ↑
Money laundering	15%	17%
AVG. Number of attacks experienced	**3**	**6** ↑

↑ = Sig. Higher for MRC Members ↓ = Sig. Lower for MRC Members

In Figure 21, we drill into this data a bit more to display the top five most prevalent forms of fraud faced by merchants in each geographic region and size segment. Comparing this year's data to last year's, the incidence of phishing / pharming / whaling attacks rose spiked significantly among merchants in Europe and APAC, as well as among mid-market merchants, in general.
There was also a significant year-over-year increase in the incidence of friendly fraud affecting enterprise merchants.

Looking at differences in fraud attacks across merchant segments, Figure 21 shows that APAC merchants are more likely than those in other regions to experience both identity theft and loyalty fraud. On the right side of the graphic, there is also a clear pattern indicating that SMBs are significantly less likely to experience most forms of fraud, while the converse is true for enterprise merchants. This pattern is similar to the one between MRC and non-MRC members highlighted in Figure 20, in that the difference in fraud rates for SMBs and enterprises may be due to enterprises suffering more attacks, to enterprises having more tools and techniques in place to help them recognize and register attacks, or to some combination of the two.

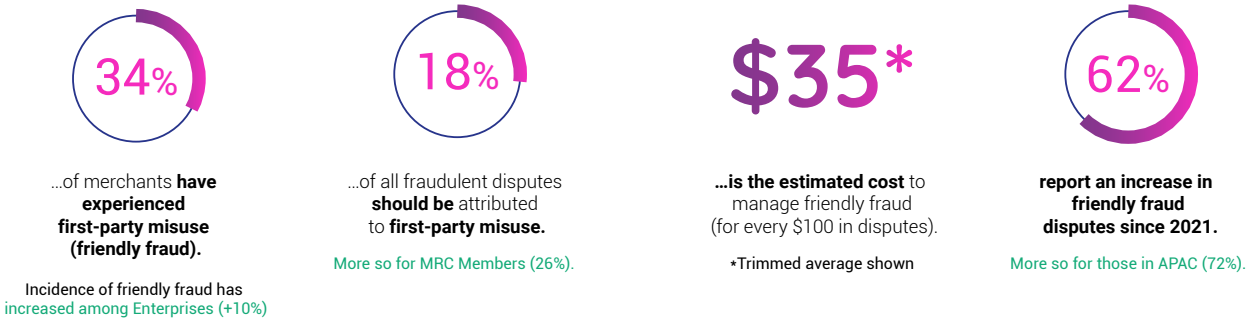
Figure 21: Top Forms Of Fraud Experienced By Region & Size Segment (2023)



Friendly Fraud Still A Pervasive Problem, But Merchants Optimistic About New Solutions

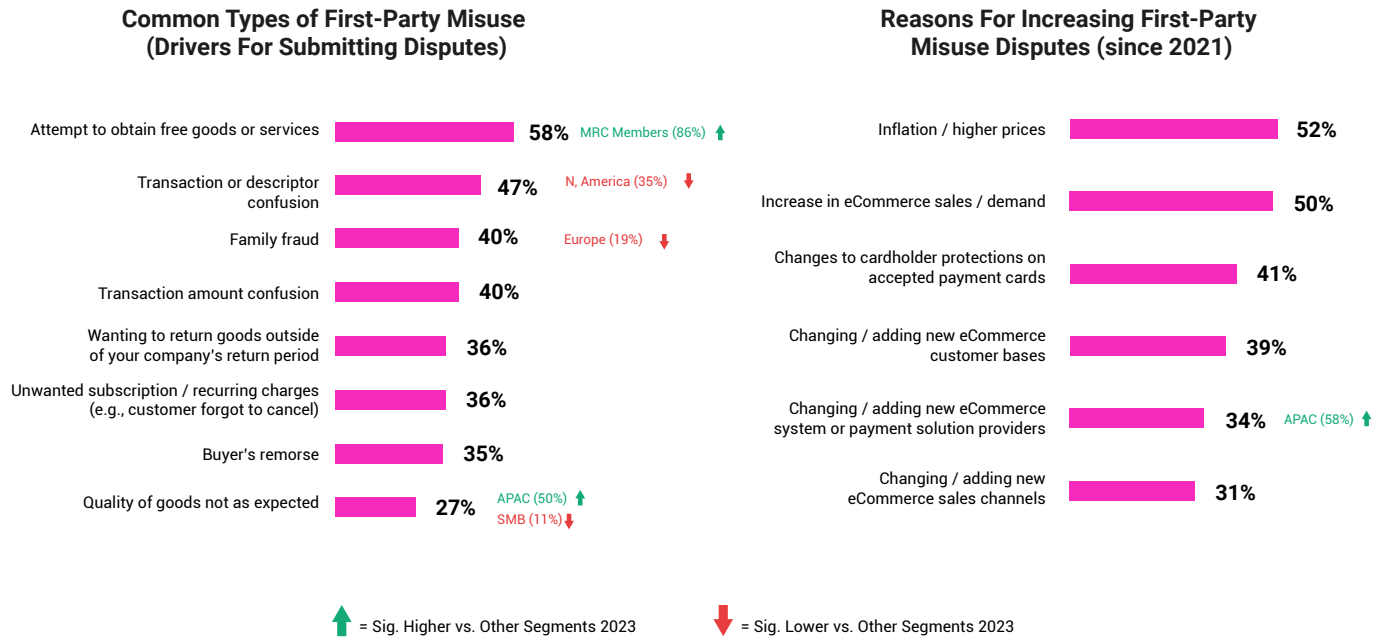
First-party misuse, also called "friendly fraud" or chargeback fraud, affects over one-third of merchants, globally, ranking this the #2 most widespread type of fraud tracked by our survey. Merchants estimate that nearly one-fifth of all fraudulent disputes should be attributed to friendly fraud, and over 6 in 10 have reported an increase in first-party misuse disputes since 2021 (see Figure 22). This form of fraud is also especially costly to combat, with merchants estimating they have to spend (USD) $35 to manage friendly fraud for every $100 they face in disputes.

Figure 22: Key Statistics Concerning First-Party Misuse (Friendly Fraud)



To some extent, the regular occurrence and recent increases in friendly fraud attempts lies beyond merchants' control, as illustrated by the data in Figure 23, showing the top drivers of friendly fraud disputes (on the left), as well as the top reasons why this type of fraud has increased over the past few years (on the right). There will always be some proportion of customers who fraudulently attempt to obtain free goods in this manner, and merchants can do little to tamp down macroeconomic inflation / higher prices and the steady, global increase in ecommerce sales or demand that they think is spurring the recent rise in first-party misuse.

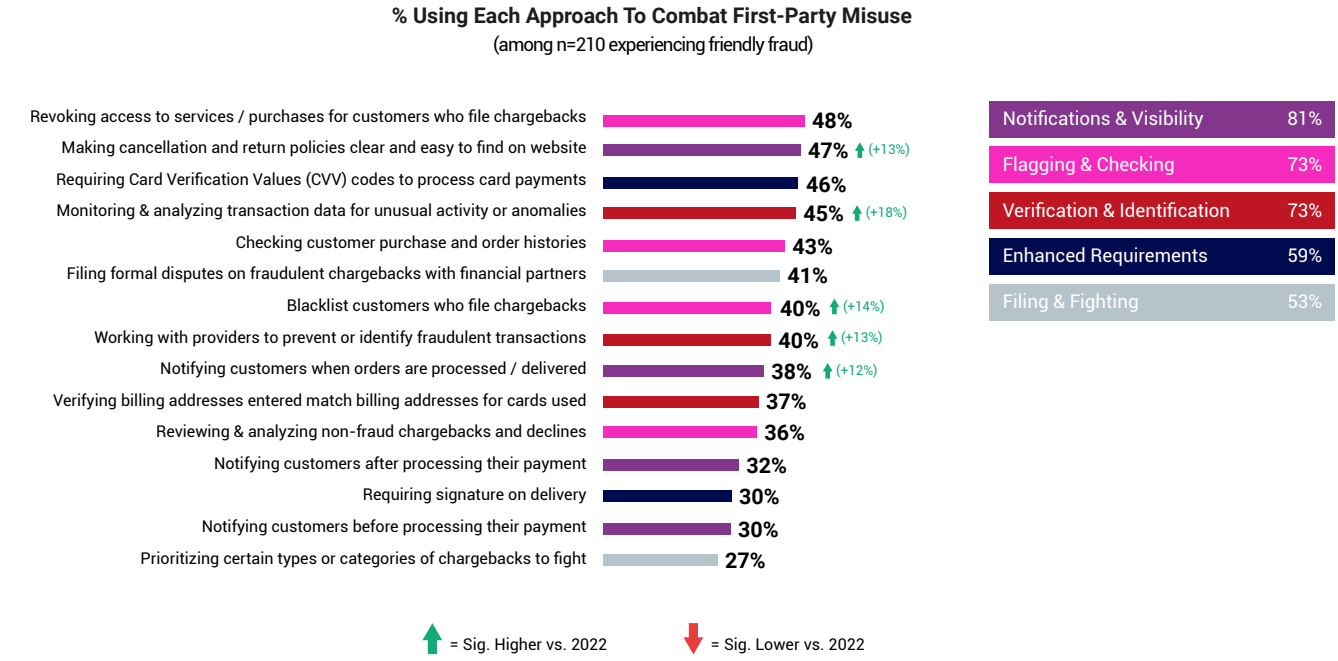
Figure 23: Drivers Of First-Party Misuse And Reasons For Rising Incidence Since 2021



This is not to say, though, that merchants are powerless to prevent or reduce friendly fraud. In fact, they are advancing quickly to implement a range of key strategies and tactics aimed at thwarting first-party misuse, and most are optimistic that recent changes to card brands' compelling evidence rules will help them to further mitigate this pernicious problem.

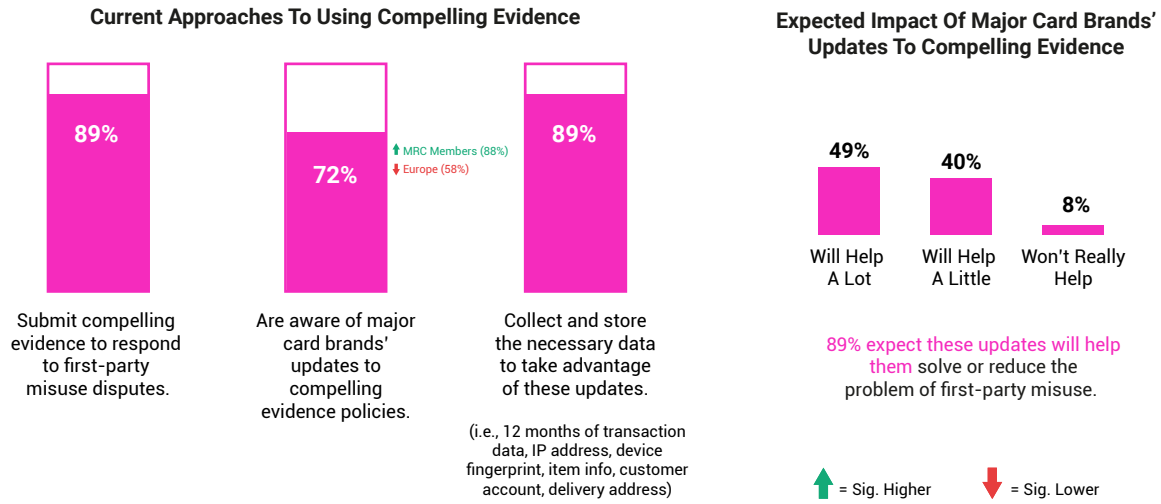
Merchants' top strategies and tactics for combating friendly fraud are shown in Figure 24. As indicated by the green arrows in the graphic, there has been a significant increase in the share of merchants leveraging multiple key tactics and techniques aimed at mitigating this form of fraud, such as making return and cancellation policies clearer and easier to find, monitoring transaction data for unusual activity, blacklisting customers who file chargebacks and working more closely with payment and fraud providers to identity and prevent friendly fraud attempts.

Figure 24: Strategies And Tactics For Tackling First-Party Misuse (Friendly Fraud)



Beyond embracing a broader array of friendly fraud-fighting tactics and techniques, merchants are also making great use of card brands' compelling evidence rules to combat this issue. Around 9 in 10 currently submit compelling evidence to resolve these types of disputes, and nearly three-quarters (72%) are already aware of major card brands' recent updates to compelling evidence rules, which are aimed at helping merchants tackle this issue more effectively (see Figure 25). Among those in the know, the vast majority – 89% – expect these recent rule updates to help them solve or reduce the problem of friendly fraud.

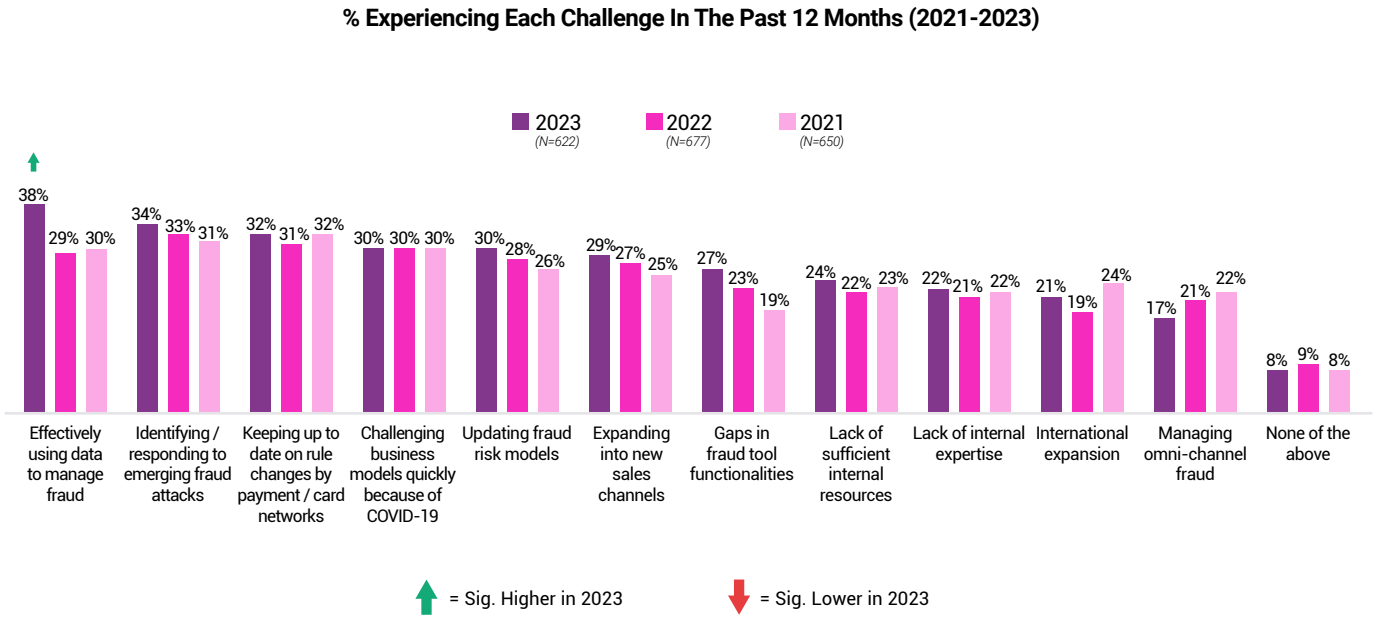
Figure 25: Usage Of Compelling Evidence To Mitigate The Problem Of First-Party Misuse



Making Better Use Of Data & Analytics To Manage Fraud Is Now A Top Priority

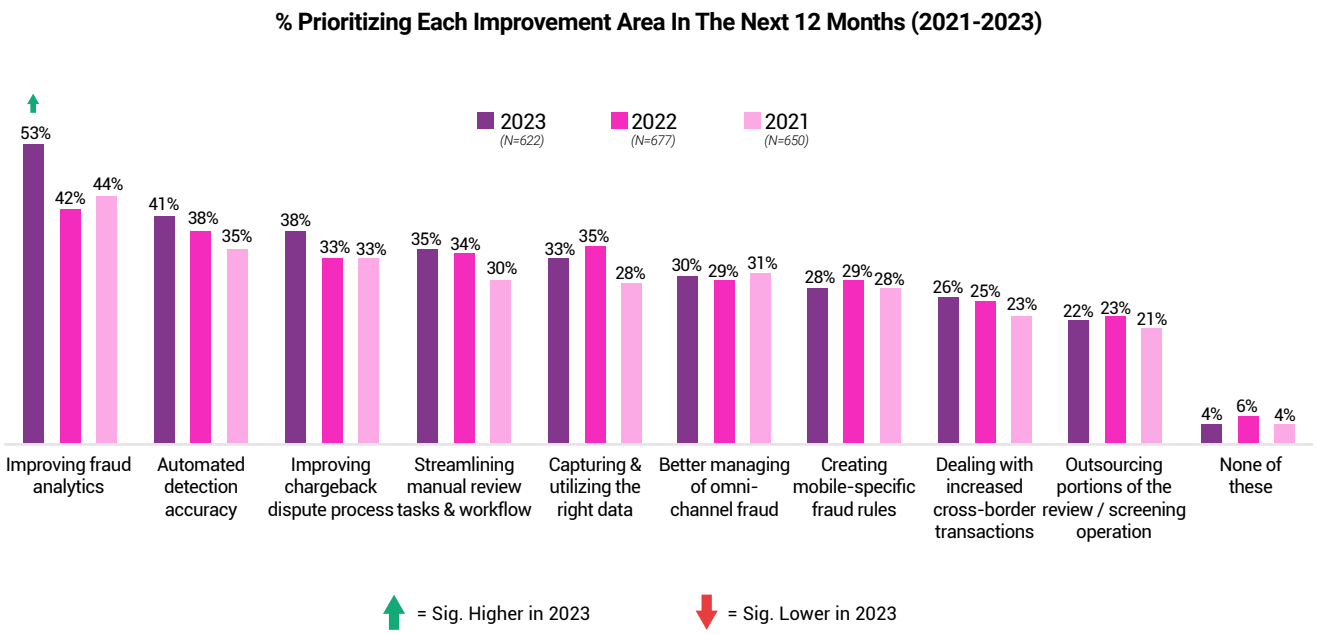
In addition to identifying, preventing and mitigating various forms of fraud at the tactical level, merchants must also manage a wide array of strategic fraud management challenges and priorities. As the data in Figure 26 illustrate, challenges related to fraud management have steadily grown for merchants, globally, over the past three years.

Figure 26: Top Challenges In Managing Ecommerce Fraud



As challenges have increased, so too have merchants' needs to make improvements in a range of strategic solutions and capabilities related to fraud management. This dynamic is reflected in the data in Figure 27, below, which shows a strikingly similar pattern to the data in Figure 26. What's clear and noteworthy at a high level from these two trends over the past three years is that both challenges and opportunities for improvement related to ecommerce fraud management are steadily increasing from merchants' point of view.

Figure 27: Top Areas For Improvement In Managing Ecommerce Fraud



At a higher level, these data highlight how one particular type of fraud-related challenge has recently become much more salient to a large swath of merchants around the world over the past few years, and that is the usage of data and analytics to more effectively manage and combat fraud. Ideally, ecommerce merchants and their payments and fraud partners can make use of the insights and analysis reported in this study, and others like it, to help address this growing need. As the complexities of fraud, global ecommerce, compliance and consumer behavior changes, the use of insights to better understand how effectively they are at managing fraud and increasing revenue remains more important than ever.

Moreover, this trend reflects a broader theme evident throughout this year's report of ecommerce merchants needing and trying to better leverage technology in their management of both ecommerce payments and ecommerce fraud. In many questions throughout our survey, we saw significant spikes in the share of merchants making use of more sophisticated technologies, such as automation, artificial intelligence, machine learning, along with the massive streams of relevant data and analytics that support and feed these advanced solutions.

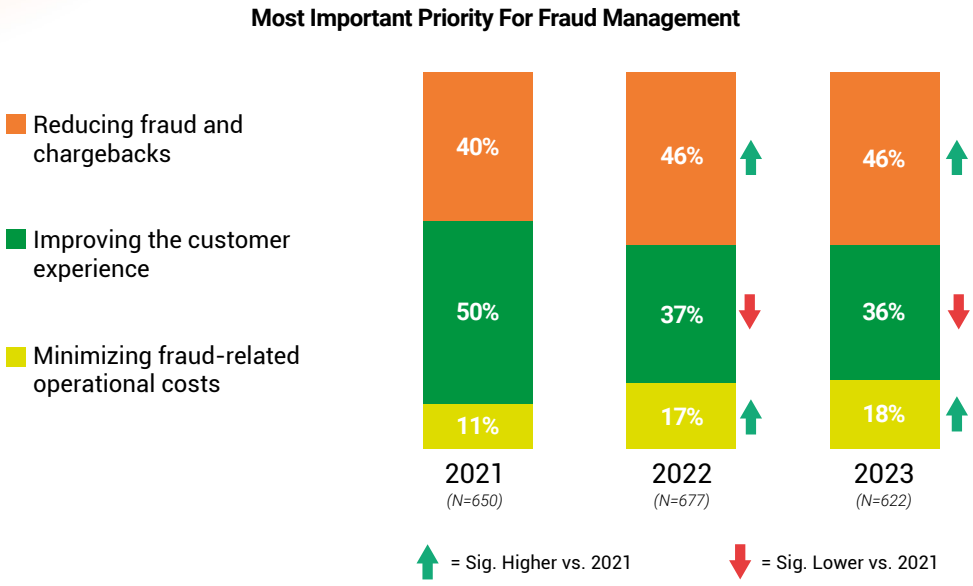
5. Fraud Prevention

The final section in this year's report examines how merchants are moving to prevent ecommerce fraud at both the strategic and tactical levels. First, we examine merchants' overall fraud management priorities and how those have evolved over time. Then we review which fraud prevention tools and tactics merchants are using and how effective those are, as well as which additional tools merchants are most likely to invest in, moving forward.

Reducing Fraud & Chargebacks Remains #1 Priority Guiding Fraud Prevention Strategies

Continuing a trend from last year's survey, when it comes to the top priority guiding merchants' fraud management strategies, they are still most likely to prioritize preventing fraud and chargebacks, versus improving CX (customer experience) or minimizing costs (see Figure 28). This strategic approach is generally consistent across merchants in different regions and size segments, although those based in Latin America show a more equal split on this question, with 40% citing CX improvement as their primary imperative and 39% citing fraud and chargeback reduction.

Figure 28: Top Priority Guiding Fraud Management Strategy – 2021-2023



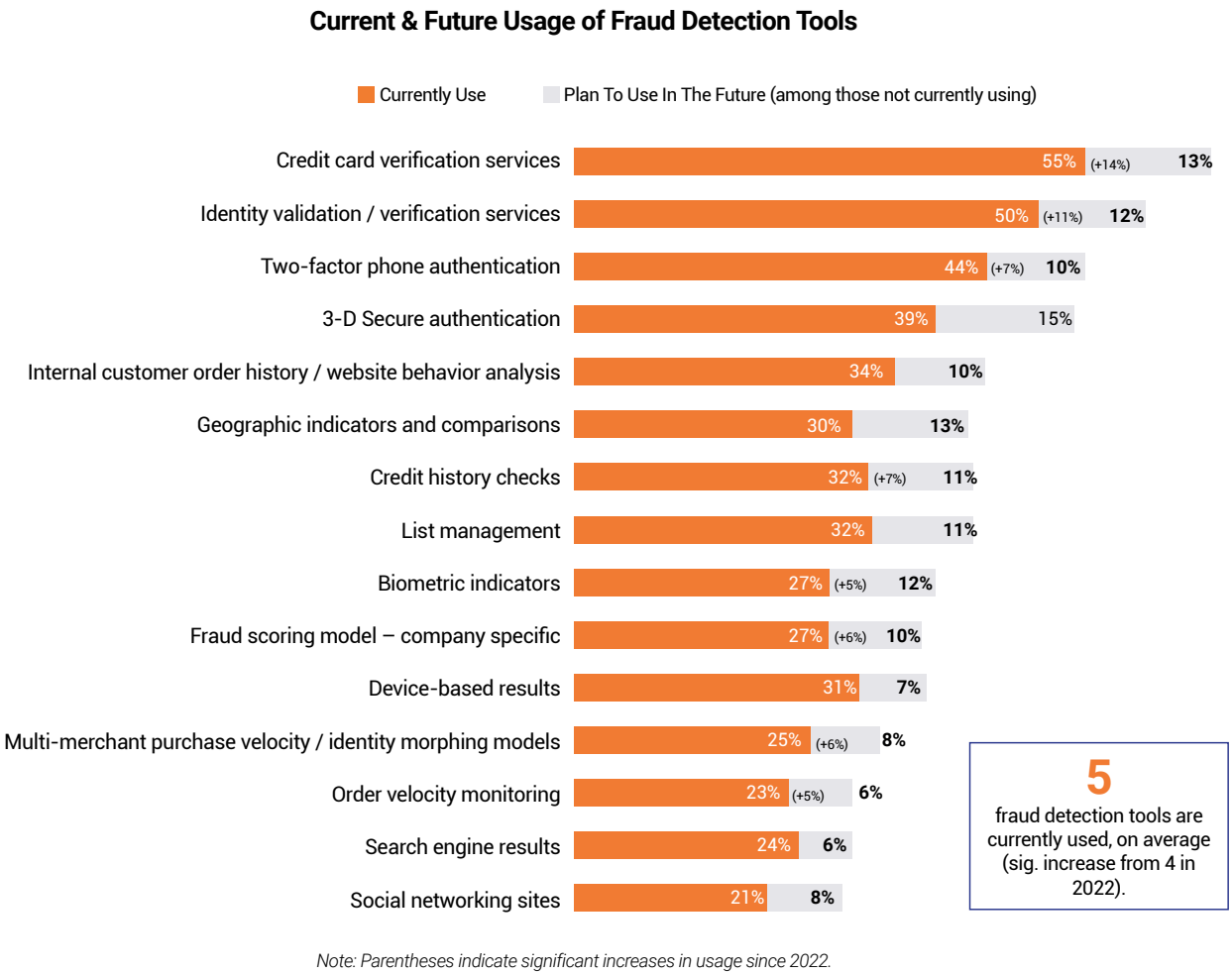
The fact that this year's survey showed significant improvement in many important fraud KPIs may be evidence that merchants' sustained focus on fraud and chargeback reduction is starting to bear fruit (see Figure 13). Moving forward, merchants will ideally be looking to continue gaining ground in the fight against fraud while maintaining strong CX and keeping costs in check.

Merchants Utilizing An Increasing Array Of Fraud Prevention Tools

Shifting from merchants' strategic priorities to the tactical tools they rely on to detect and prevent fraud, the survey shows a significant increase in the average number of tools currently in use, from four last year to five this year. Eight out of the 15 different tools tracked by the survey registered a significant uptick in usage by merchants, globally, over the past year (see Figure 29).

These include the three most widely used tools (credit card verification services, identity verification services and two-factor phone authentication), as well as a handful of tools used by one-quarter to one-third of all merchants (credit history checks, biometric indicators, fraud scoring models, multi-merchant purchase velocity models, and order velocity monitoring). In general, the tools showing the biggest increases in usage over the past year are also the ones selected by the largest shares of non-users as tools they plan to adopt in the future.

Figure 29: Current & Planned Usage Of Fraud Detection Tools

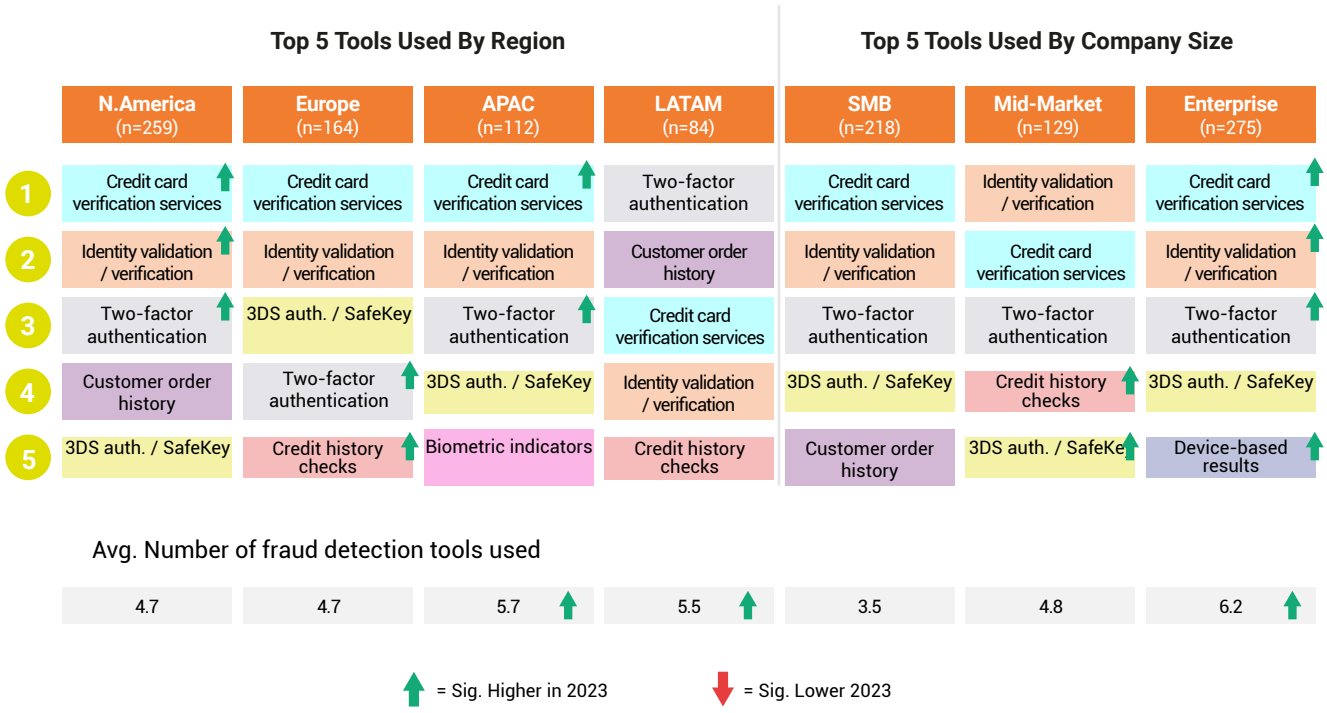


Note: Parentheses indicate significant increases in usage since 2022.

Figure 30, below, shows the top five tools used by merchants in each region and size segment, as well as which tools were implemented by a significantly larger share of merchants in each segment over the past year. As indicated by the green arrows in each column of the graphic, merchants in almost every segment significantly increased their usage of at least one of these top tools, with merchants in North America and enterprises reporting increased usage of most of them. The figures at the bottom of Figure 30 highlight how APAC and LATAM-based merchants, as well as enterprises, use significantly more tools than those in other segments.

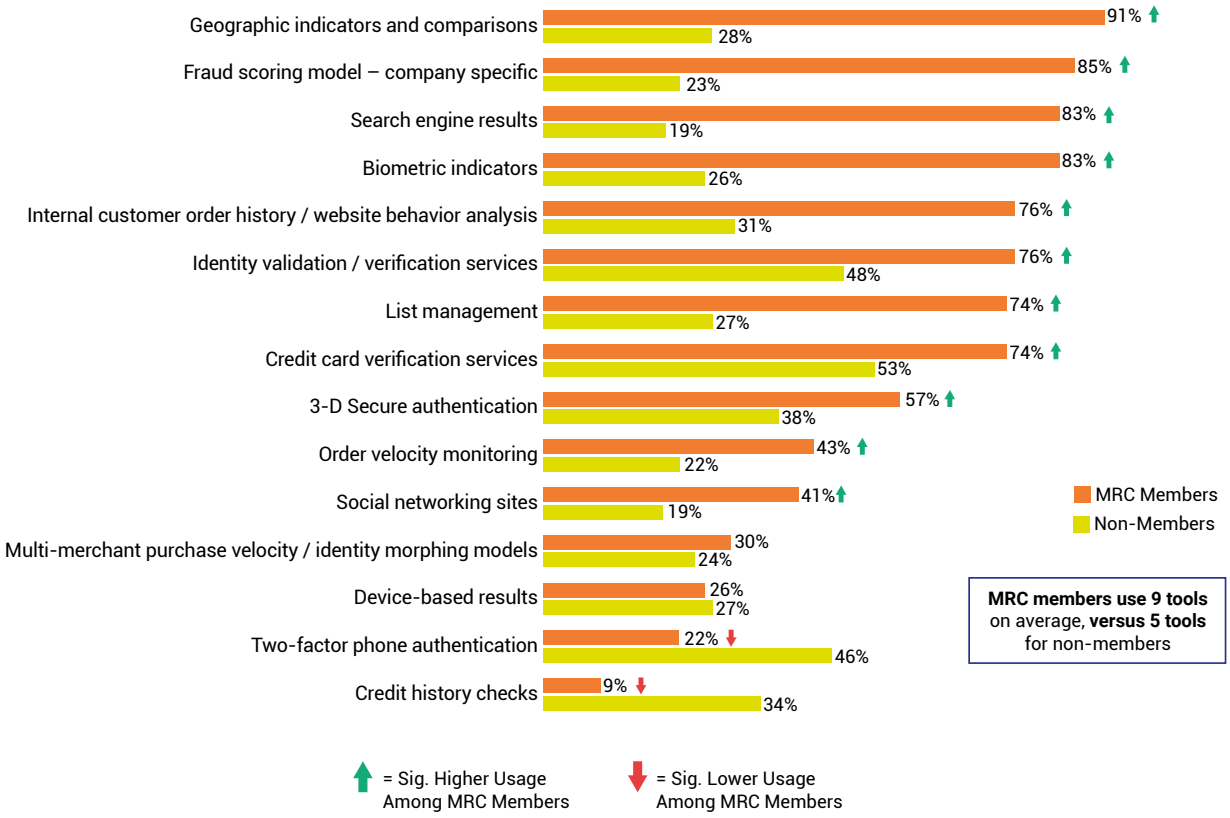
The data in Figure 30 once again underscore a bit of recent rebalancing on merchants' part toward applying "best practice" tools like two-factor authentication and identity verification, versus more sophisticated tools supported by artificial intelligence or machine learning algorithms.

Figure 30: Top 5 Fraud Detection Tools Used By Region & Size (2023)



Consistent with past years of this survey, MRC members continue to use a much larger array of fraud detection and prevention tools than non-members: nine, on average, versus five among non-members (see Figure 31). This dynamic may be driven in part by the fact that 6 in 10 MRC members currently outsource fraud tools, while only 35% of non-members do the same.

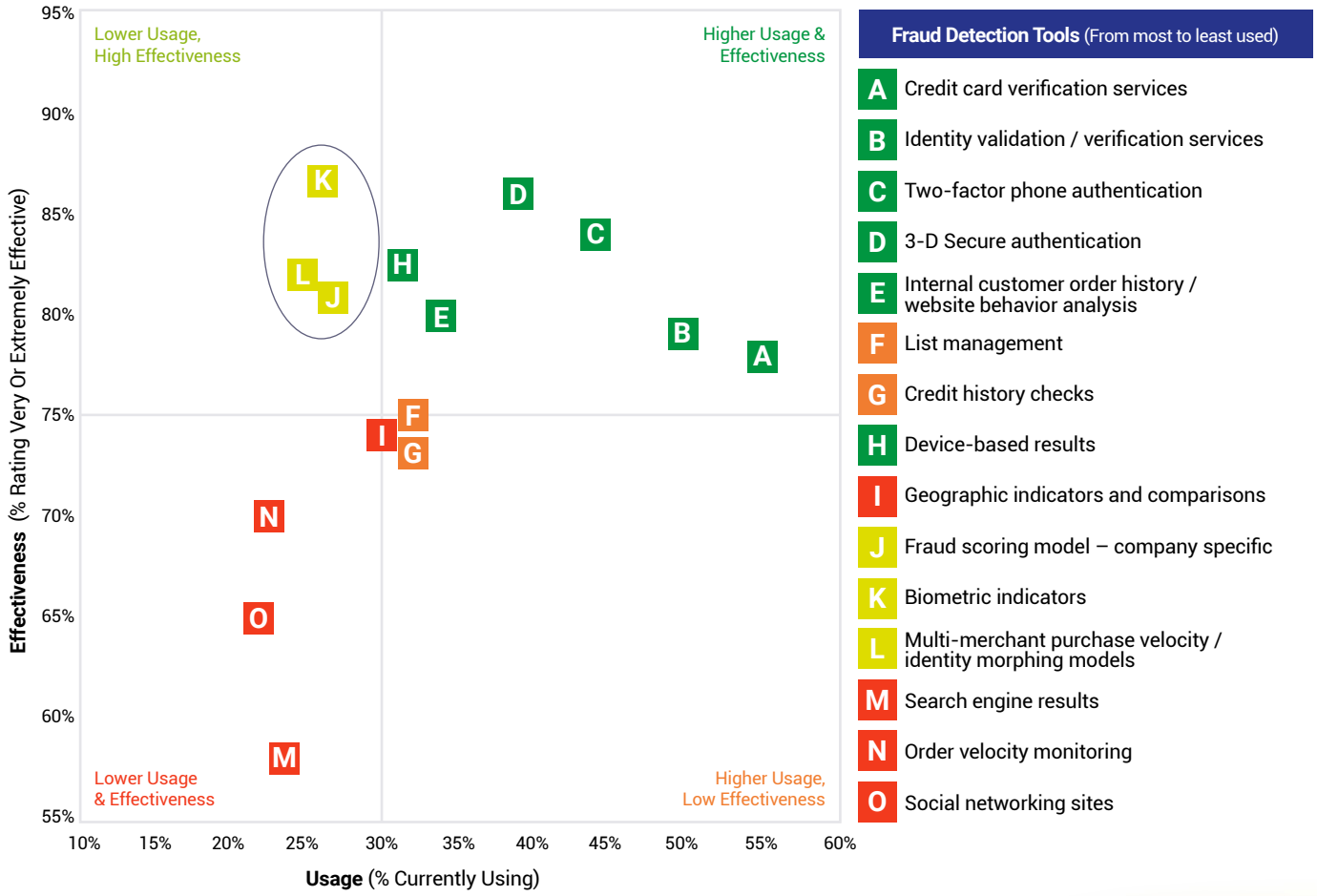
Figure 31: Usage Of Fraud Detection Tools Among MRC Members vs. Non-Members (2023)



Most Effective Tools Are Generally Used Most Widely, With A Few Notable Exceptions

As merchants have adopted and implemented more fraud prevention tools in recent years, they have generally been successful at choosing the ones that are most effective. The data in Figure 32 reflect this good overall correlation between tool usage and effectiveness. There are a few notable exceptions, however, which might help inform future adoption and investment plans for merchants: fraud scoring models, biometric indicators, and multi-merchant purchase velocity / identity morphing models are all seen as highly effective but have yet to be widely adopted.

Figure 32: Usage Vs. Effectiveness Of Fraud Detection Tools



Conclusion

The insights and findings captured in this year's survey paint a vivid and encouraging picture of how ecommerce merchants are managing payments and fraud, globally. At a high level, merchants are clearly making meaningful progress and advancement in their approaches to both payments and fraud management.

They are offering customers a wider range of payment methods, such as BNPL and local digital payments, making increased use of sophisticated technologies to innovate and improve payment and retail experience (e.g., AI chatbots and connected devices), utilizing multiple marketplace, processor and acquirer partners to optimize both customer-facing and back-end payment processes, and tracking an increasing array of payment metrics and KPIs, so they can further enhance and optimize their payment strategies, in the future.

When it comes to managing and mitigating ecommerce fraud, merchants' steady strategic focus on reducing fraud and chargebacks and their consistent, robust spending on fraud management is paying quantifiable dividends in the form of significantly improved fraud KPIs. They are tackling thorny issues like friendly fraud head-on, collaborating with payment partners to quickly introduce new anti-fraud processes and solutions, and investing in a steadily expanding arsenal of anti-fraud tools and technologies.

Fraudsters are always looking for the next opportunity to find a hole in the process, and merchants will always have more work to do and new problems to face when it comes to preventing fraud. And, with consumer demands ever-changing at a rapid pace, managing ecommerce payments can also be challenging for merchants. But the data and trends in this year's report provide good reason for optimism that they can continue to advance and achieve success in both of these challenging arenas.

About the authors

Cybersource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast $427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues and mitigating risk. For acquirer partners, Cybersource provides a technology platform, payments expertise and support services that help them grow and manage their merchant portfolio to fulfil their brand promise.

For more information, please visit: cybersource.com

Merchant Risk Council (MRC) is a non-profit global membership organization connecting eCommerce fraud prevention and payments professionals through educational programs, online community groups, conferences, and networking events. Encompassing 600+ companies, including 400+ merchants, it provides education on fraud prevention, payments optimization, and risk management. The MRC was established in 2000 and continues to be at the forefront of industry evolution by focusing its efforts on optimizing payments and reducing eCommerce fraud through collaboration, networking, education, and advocacy.

For more information, please visit: merchantriskcouncil.org

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 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 a consortium of world-class B2B agencies who came together to form Merkle B2B. Being a Merkle B2B company allows us to deliver the world's first end-to-end, fully-integrated B2B solution. Our one promise? To architect the ultimate B2B customer experiences.

For more information, please visit: b2binternational.com

Appendix 1 – Conversion and Acceptance Rates By Payment Method

This section displays the average (mean and median) conversion and acceptance rates by payment method, as reported by merchants in this year's survey.

Card, direct debit and digital wallet payments have the highest average conversion rates, with means ranging from 25 to 40 percent, globally. Conversion rates are significantly lower for bank / debit transfer and for digital wallet payments in Latin America (see Figure 33).

Figure 33

Average conversion rates by payment method (median/*mean*)

	Overall	North America	Europe	APAC	LATAM	SMB	Mid-Market	Enterprise
Cards	30% *38%*	35% *43%*	35% *40%*	25% *33%*	25% *31%*	34% *39%*	30% *36%*	30% *38%*
Bank transfers / direct debit	20% *30%*	25% *33%*	30% *37%*	20% *28%*	20% *19%*↓	20% *29%*	25% *33%*	20% *29%*
Digital wallets / eWallets	20% *26%*	20% *27%*	20% *30%*	28% *29%*	15%↓ *18%*↓	20% *26%*	20% *25%*	20% *27%*
Cash on delivery	15% *23%*	10% *22%*	18% *27%*	20% *27%*	10% *16%*	10% *22%*	15% *26%*	16% *23%*
mCommerce mobile payments	15% *22%*	20% *24%*	15% *23%*	20% *24%*	15% *18%*	15% *20%*	15% *24%*	20% *23%*
Buy Now Pay Later	15% *20%*	15% *20%*	15% *22%*	10% *19%*	10% *15%*	12% *16%*	10% *21%*	15% *21%*
Gift cards / vouchers	10% *19%*	10% *21%*	10% *17%*	10% *21%*	10% *13%*	10% *16%*	10% *20%*	10% *20%*
Cryptocurrency	10% *15%*	10% *17%*	10% *17%*	13% *16%*	7% *9%*	10% *15%*	10% *16%*	10% *16%*
Other local digital payments	11% *17%*	12% *16%*	10% *14%*	10% *18%*	20% *21%*	10% *16%*	10% *20%*	15% *17%*

(All means calculated with trimmed averages)

↓ Sig. Lower vs. Other Segments

When it comes to payment acceptance, the same three methods – cards, debit transfers, and digital wallets – also show the highest average rates, with means ranging from 30 to 50 percent (see Figure 34).

Figure 34

Average acceptance rates by payment method (median/*mean*)

	Overall	North America	Europe	APAC	LATAM	SMB	Mid-Market	Enterprise
Cards	50% *55%*	75% *62%*	60% *58%*	40% *46%*	40% *46%*	50% *56%*	50% *53%*	50% *56%*
Bank transfers / direct debit	35% *47%*	40% *50%*	50% *55%*	25% *42%*	21% *34%*	40% *48%*	40% *51%*	30% *44%*
Digital wallets / eWallets	30% *44%*	30% *46%*	38% *50%*	30% *41%*	20% *32%*	30% *44%*	30% *47%*	30% *42%*
Cash on delivery	20% *38%*	14% *34%*	30% *46%*	27% *41%*	15% *29%*	18% *38%*	25% *36%*	20% *38%*
mCommerce mobile payments	25% *40%*	30% *42%*	33% *44%*	25% *37%*	20% *32%*	25% *40%*	25% *44%*	27% *37%*
Buy Now Pay Later	20% *36%*	25% *35%*	30% *42%*	20% *32%*	15% *29%*	20% *34%*	25% *38%*	20% *35%*
Gift cards / vouchers	20% *38%*	20% *37%*	20% *42%*	20% *38%*	10% *30%*	11% *34%*	20% *37%*	20% *40%*
Cryptocurrency	20% *28%*	20% *31%*	23% *36%*	18% *21%*	10% *18%*	15% *31%*	15% *27%*	20% *26%*
Other local digital payments	20% *35%*	20% *27%*	24% *41%*	23% *31%*	23% *36%*	20% *36%*	20% *39%*	20% *32%*

(All means calculated with trimmed averages)

Appendix 2 – questions asked

This section shows the questions asked to survey respondents to gather the data shown 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 the primary source of your eCommerce revenue?

Figures 4, 5 & 6

- 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 7

- In what ways, if any, does your organization encourage or guide customers to use your preferred types of payment method(s)?
- What is the ONE most important reason why you encourage customers to use your preferred payment method(s)?

Figure 8

- Which, if any, of the following third-party marketplaces does your organization currently use to sell to customers?
- Why does your organization utilize third-party marketplaces?

Figure 9

- 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 10

- Which, if any, of the following retail approaches are used by your organization?
- Which, if any, of the following customer experiences does your organization currently offer?

Figure 11

- Which, if any, 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 12

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

Figure 13

- Please indicate the percent of your annual eCommerce revenue lost due to payment fraud globally, i.e., fraud rate by revenue. This includes fraud chargebacks received, as well as credits or refunds issued directly to customers who claim not to have placed an order as well as chargeback fees.
- Please indicate the percent of your annual eCommerce revenue lost due to payment fraud on orders from [INSERT COUNTRY], i.e.,

domestic orders. This includes fraud chargebacks received, as well as credits or refunds issued directly to customers who claim not to have placed an order as well as chargeback fees. Your best estimate is fine.

- Please indicate the percent of accepted annual eCommerce orders that turned out to be fraudulent (i.e., fraud rate by order) from [INSERT COUNTRY] i.e. domestic orders.
- Please indicate the percent of accepted annual eCommerce orders that turned out to be fraudulent (i.e., fraud rate by order) from outside INSERT COUNTRY] i.e. international orders.
- Please indicate the percent of eCommerce orders for which you have received chargebacks due to fraud. Note: A chargeback is defined as a transaction where the card issuing back disputes a previously authorized transaction.
- Please indicate your order rejection rate for domestic orders.
- Please indicate your order rejection rate for international orders.

Figure 14

- Please indicate the percent of your annual eCommerce revenue your organization spends to manage payment fraud — excluding actual fraud losses.

Figure 15

- How do your organization's future fraud strategy plans incorporate manual review?

Figure 16

- Please indicate the percentage of eCommerce orders you manually screen for fraud.
- Of the eCommerce orders manually reviewed by your organization, please indicate the percentage you decline (cancel) due to suspicion of fraud.

Figure 17

- To what extent has your organization implemented changes necessary to comply with PSD2, in particular, strong customer authentication (SCA)?

Figure 18

- And how do you expect PSD2, in particular, strong customer authentication (SCA), to impact your organization?
- With respect to SCA, how many of the following exemptions or out-of-scope flags are you planning on utilizing in the future?

Figure 19, 20 & 21

- Which of the following types of fraud attacks, if any, have you ever experienced at your organization?

Figure 22

- Which of the following types of fraud attacks, if any, have you ever experienced at your organization?
- Has your organization experienced an increase in first-party misuse / friendly fraud disputes since 2021?
- Approximately how much does it cost your organization to manage first-party misuse / friendly fraud disputes (for every $100 in disputes)?
- What percentage of (all) fraudulent disputes do you believe are first-party misuse (i.e., friendly fraud or chargeback fraud)?

Figure 23

- For what reasons do you believe your organization has seen an increase in first-party misuse / friendly fraud disputes since 2021?
- Which of the following reasons do you believe causes first-party misuse (i.e., friendly fraud or chargeback fraud) to occur at your company?

Figure 24

- Which of these describe your organization's current approach to combating First-Party Misuse (i.e., friendly fraud / chargeback fraud)?

Figure 25

- Do you submit compelling evidence to respond to first-party misuse / friendly fraud disputes?
- Have you heard of major card brands' updates to compelling evidence (related to first-party misuse / friendly fraud disputes)?
- Do you believe these updates will help solve or reduce the problem of first-party misuse / friendly fraud?
- Do you collect and store the necessary data elements on historical transactions to take advantage of these updates?

Figure 26

- Which of the following challenges related to eCommerce fraud management, if any, has your organization experienced in the last 12 months?

Figure 27

- Thinking ahead to the next 12 months, which of the following, if any, are areas of improvement for your organization?

Figure 28

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

Figure 29

- Next is a series of fraud detection tools. Please indicate which tools your organization currently uses.
- Which tools, if any, does your organization have plans to start using in the future?

Figure 30 & 31

- Next is a series of fraud detection tools. Please indicate which tools your organization currently uses.

Figure 32

- Next is a series of fraud detection tools. Please indicate which tools your organization currently uses.
- Now, how effective is each of the following tools in detecting eCommerce payment fraud?

Figure 33

- What is your organization's average conversion rate (i.e., percentage of visits from the checkout page that result in a completed checkout) for each of the following payment methods that you currently accept?

Figure 34

- Please estimate your organization's acceptance rate (meaning the percentage of initiated payments accepted by the payment provider) for each of the following types of payment methods.