



Global fraud and payments report 2022



cybersource
A Visa Solution

Report contents

03	Disclaimer
04	Overview
05	Executive summary
08	Survey firmographics
09	Business impact of fraud: key findings
14	Range of fraud attacks: key findings
19	Fraud prevention: key findings
22	Payment acceptance and partners: key findings
27	Payment management: key findings
32	About the authors
33	Appendix 1 – conversion and acceptance rates by payment method
34	Appendix 2 – questions asked in the survey

Disclaimer

Case studies, comparisons, statistics, research, and recommendations are provided “AS IS” and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

Studies, survey results, research, recommendations, and opportunity assessments are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory, or other advice. Recommendations and opportunities should be independently evaluated considering your specific business needs and any applicable laws and regulations. Cybersource is not responsible for your use of any studies, survey results, research, recommendations, opportunity assessments, or other information, including errors of any kind, or any assumptions or conclusions you might draw from their use. Except where statistically significant differences are specifically noted, survey results should be considered directional only. Neither Cybersource, nor any of its employees, subsidiaries, parents, or affiliates make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information disclosed herein.

Overview

Cybersource, the Merchant Risk Council (MRC), and Verifi are pleased to present the results of the 2022 Global Fraud and Payments Survey, a report that conveys transparent and unbiased research. This report is based on a survey of merchants from around the globe, who were asked about their eCommerce fraud and payments practices. The survey sample included 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. The research was conducted in November and December of 2021.

The survey results provide the 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 merchants can use to help optimize their fraud management and prevention practices. In addition, the survey delves into today's rapidly changing payments landscape to examine the range of different payment acceptance, management and partnership practices merchants are deploying, globally and across key subsegments, as well as the reasons why they are adopting these payment strategies and tactics in the current commercial environment.

Cybersource would like to thank the participants for taking the time to complete the online survey, the MRC and Verifi for their continued partnership, and B2B International for directing the program and providing the analysis.

Executive summary

The key findings from the 2022 Fraud and Payments survey are organized into five focus areas. Each area covers a central question integral to understanding the state of eCommerce fraud and payments from the merchant perspective.

The first three focus areas cover questions related to eCommerce fraud, specifically:

01

What effect is fraud having on merchant businesses today?

02

What types of fraud attacks are merchants experiencing?

03

What strategic and tactical approaches are merchants using to prevent and manage fraud?

The final two focus areas delve into questions related to eCommerce payments, specifically:

04

What practices and partners are merchants using to accept eCommerce payments?

05

How are merchants optimizing payment processes and platforms?

The key, high-level insights from each of the five focus areas are summarized below:



1. Business impacts of fraud – what are the effects of fraud?

- Globally, fraud costs and KPIs all increased (or worsened) for a second consecutive year, yet most merchants did not increase the share of revenue they spend to manage fraud. Merchants in North America were the only segment to increase fraud management spending, likely due, in part, to the significant upticks they registered in costs and KPIs.
- Most merchants still seek to reduce dependency on manual order review, and this aim may now be translating to action, given slight decreases this year in the share of orders manually reviewed and the share of reviewed orders that are ultimately rejected.
- Merchants generally feel well-prepared for the revised Payment Services Directive, specifically related to the implementation of Strong Customer Authentication (known as PSD2 SCA) and for the implementation of EMV® 3DS – new requirements being implemented in European Economic Area (EEA) that will collectively bolster anti-fraud postures. It's worth noting that all EEA markets have now reached full SCA enforcement.



2. Range of fraud attacks – where are merchants most vulnerable?

- Phishing / pharming, card testing, identity theft, and first-party misuse remain the most prevalent fraud attacks, each affecting more than 3 in 10 merchants globally.
- Globally, on average, merchants believe 16% of fraudulent disputes should be attributed to first-party misuse (or “friendly fraud”), with the majority of disputed transactions a result of issues with cardholders aiming to obtain free goods, confusion about transaction descriptors, or issuers incorrectly filing disputed transactions as fraud. In some regions and sectors, merchant estimates for this figure ranged as high as 1 in 5.
- 9-in-10 merchants have experienced at least one fraud management challenge and merchants are struggling to overcome three challenges, on average. The most pervasive and impactful challenges are identifying & responding to fraud attacks, changing business models because of COVID, & expanding into new sales channels



3. Fraud prevention strategies – How are merchants addressing the issue of eCommerce fraud?

- The top priority driving fraud management strategies changed over the past year: More merchants now prioritize reducing fraud and chargebacks as their primary imperative, versus optimizing the customer experience, which was the main goal for most in 2021. In part, this strategic shift may be driven by rising fraud costs and KPIs.
- At the tactical level, merchants report using an average of four fraud detection tools and services, in total. Payment card and identity verification services, along with 3D-Secure and two-factor phone authentication, are the most widely used tools.



4. Payment acceptance and partners – how are merchants being paid?

- Most eCommerce merchants accept payments via digital wallets, direct debit, payment cards, and mCommerce mobile payments. The vast majority (nearly 9 in 10) encourage customers to pay via preferred methods, mainly to minimize risk of payment fraud.
- Third-party payments, buy now pay later (BNPL), digital wallet, and mobile payments are the fastest growing payment methods; most merchants who accept these added them in the past year. Improving the customer experience is the top reason merchants add new methods, but reaching new customer segments and markets, as well as “going mobile,” are important drivers too. Similar motivations also drive most to sell goods on third-party marketplaces.
- Merchants leverage multiple payment processors and acquiring banks to support omnichannel payments. Maximizing flexibility, geographic coverage, uptime, and authorizations represent merchants’ main motivations for utilizing multiple acquirers.



5. Payment management – How are merchants optimizing processes and platforms?

- Merchants are experimenting with a diverse range of novel retail approaches, such as buy now pay later (or BNPL) and buy online pickup in store (BOPIS), as well as new customer experiences to facilitate payments, like AI chatbots and face-to-pay technologies. But all of these have yet to be widely adopted. APAC, LATAM, mid-market, and enterprise merchants, are more likely to be early adopters of these new approaches and experiences.
- On average, merchants use 2 to 3 different approaches or techniques to optimize payment authorization. EMV® 3DS, intelligent routing, machine learning and automated retries are most common. Most use third-party data in association with each technique.
- Most merchants focus on 3 to 4 payment management KPIs, with payment success rate, revenue, & cost of payments comprising the top three KPIs for merchants globally.

Survey firmographics

The survey was fielded in November and December of 2021. A total of 1,060 merchants involved in eCommerce fraud and payment management participated in the research. The sample includes merchants based in four major geographic regions, with broad representation across all size tiers, sales channels and categories. The breakdown of the total merchant sample across key firmographics is depicted in the charts below.

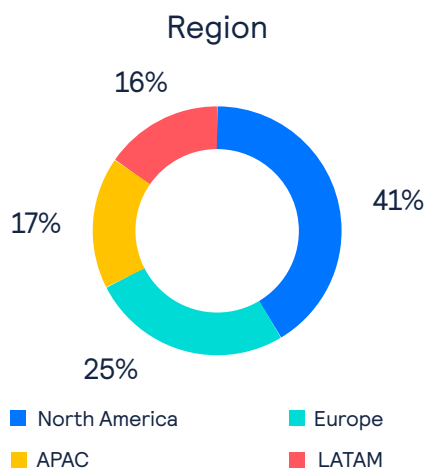


Figure 1

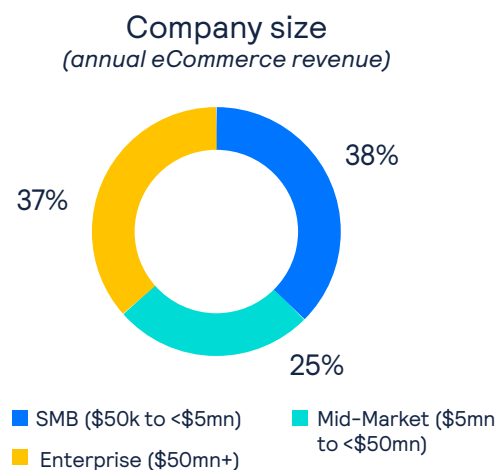


Figure 2

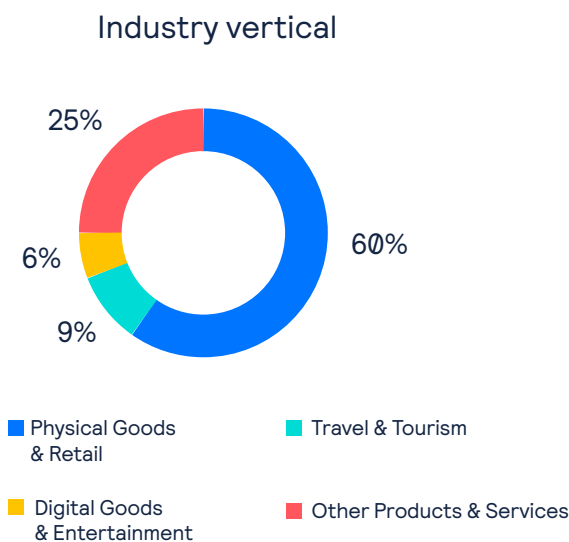


Figure 3

1. Business impact of fraud: key findings



The first section of this report focuses on how eCommerce fraud is affecting merchants, how fraud management KPIs and investments have changed over the past year, and where merchants have been successful in thwarting fraud attacks and mitigating harmful impacts. In addition, this section delves into the topic of manual order review to shed light on how integral this process is to merchant fraud management strategies, now and in the future. Lastly, this section examines merchant readiness to support PSD2 SCA and EMV® 3DS.

Fraud costs and KPIs continue to rise

For the second year in a row, merchants reported across-the-board increases in multiple key indicators that measure the extent to which fraud is impacting eCommerce. From more revenue being lost to fraud to more eCommerce orders being rejected as fraudulent to increasing chargebacks and disputes, the average figures merchants reported for every key indicator tracked in the survey increased over the past year globally, on average (see Figure 4).

Table shows fraud management KPIs
(Trimmed averages shown for all KPIs)

			By Region - 2022				By Size - 2022		
	2021	2022	North America	Europe	APAC	LATAM	SMB	Mid-market	Enterprise
% of eCommerce revenue lost to payment fraud globally	3.1	3.6	3.6 ↑ (2.6)	3.0 ↓ (3.2)	4.3 ↓ (4.0)	4.2 ↓ (3.7)	2.9 ↓ (3.0)	4.1 ↑ (3.4)	3.7 ↓ (3.0)
% of eCommerce revenue lost to payment fraud from domestic orders	3.0	3.4	3.6 ↑ (2.5)	2.8 ↓ (2.9)	3.3 ↓ (3.9)	3.6 ↓ (3.9)	3.0 ↓ (2.7)	3.8 ↑ (3.4)	3.4 ↓ (3.1)
Order rejection rate for domestic orders (%)	3.0	3.4	3.6 ↑ (2.8)	2.8 ↓ (2.8)	2.9 ↓ (3.8)	4.4 ↓ (4.0)	2.8 ↓ (2.4)	3.9 ↑ (3.7)	3.6 ↓ (3.3)
Order rejection rate for international orders (%)	5.6	6.0	6.3 ↑ (5.0)	5.1 ↓ (5.6)	5.3 ↓ (5.7)	7.0 ↓ (6.9)	5.3 ↓ (5.1)	6.7 ↑ (6.2)	6.0 ↓ (5.5)
% of domestic eCommerce orders that turned out to be fraudulent	2.6	3.1	3.2 ↑ (2.2)	2.7 ↓ (2.5)	2.9 ↓ (3.6)	3.4 ↓ (3.5)	2.6 ↓ (2.3)	3.7 ↑ (3.0)	3.1 ↓ (2.7)
% of international eCommerce orders that turned out to be fraudulent	3.0	3.4	3.3 ↑ (2.8)	3.0 ↓ (3.2)	3.7 ↑ (3.1)	4.0 ↑ (3.1)	3.0 ↓ (2.7)	3.8 ↑ (3.1)	3.3 ↓ (3.2)
% of eCommerce orders that led to chargebacks	2.7	3.1	3.4 ↑ (2.2)	2.3 ↓ (2.6)	2.9 ↓ (3.6)	3.8 ↓ (3.8)	2.6 ↓ (2.4)	3.7 ↑ (3.0)	3.3 ↓ (2.9)

↓ = Sig. Lower vs 2021

↑ = Sig. Higher vs 2021

(%=2021 figures)

(%=2021 figures)

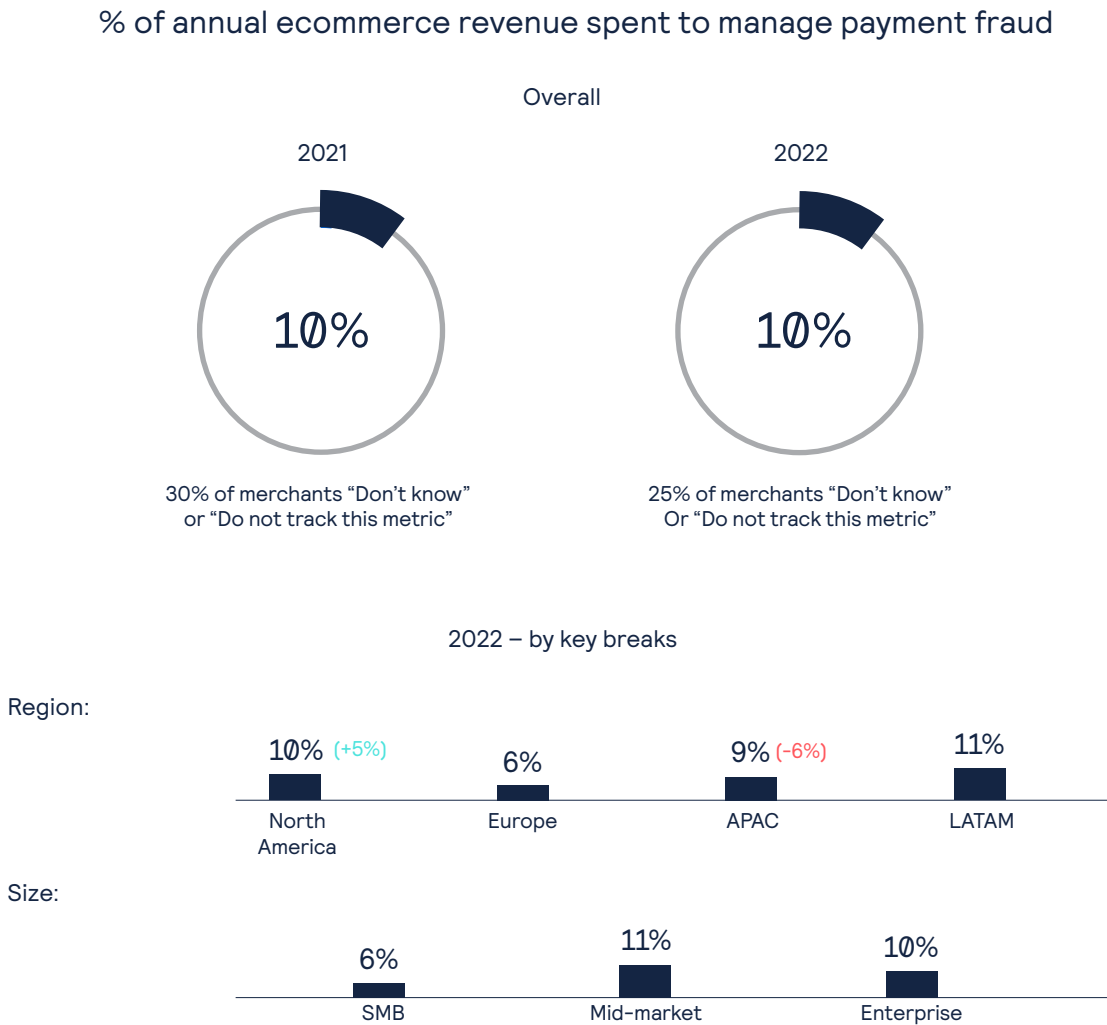
Figure 4

While the impacts of fraud have generally intensified worldwide, merchants in North America were hit particularly hard over the past year, reporting larger upticks in most fraud KPIs compared to those operating in other regions. On the other hand, merchants based in APAC saw significant declines in most fraud KPIs tracked by the survey, bringing their averages more in line with merchants in other regions, when compared to last year.

Mid-market merchants reported significant spikes across most fraud KPIs. The average values reported by mid-market merchants on every metric now exceed those of eCommerce businesses on the SMB and enterprise ends of the size spectrum. These midsize organizations may have disproportionate impacts from eCommerce fraud, as they are large enough to be appealing targets for fraudsters but have smaller budgets and fewer personnel, tools and resources to utilize for fraud prevention.

Fraud management spending stays flat

Despite rising fraud KPIs and revenue losses over the past year, merchants generally continue to spend the same amount on fraud management (as a share of total revenue). Globally, merchants spend an average of 10% of their eCommerce revenues to manage payment fraud – the same percentage recorded in 2021 (see Figure 5). While spend among most merchant segments remained consistent, North American merchants doubled the average share of revenue they allocate to fraud management, from 5% last year to 10% this year. APAC-based merchants reduced spend slightly, bringing their outlay more in line with merchants in other regions.

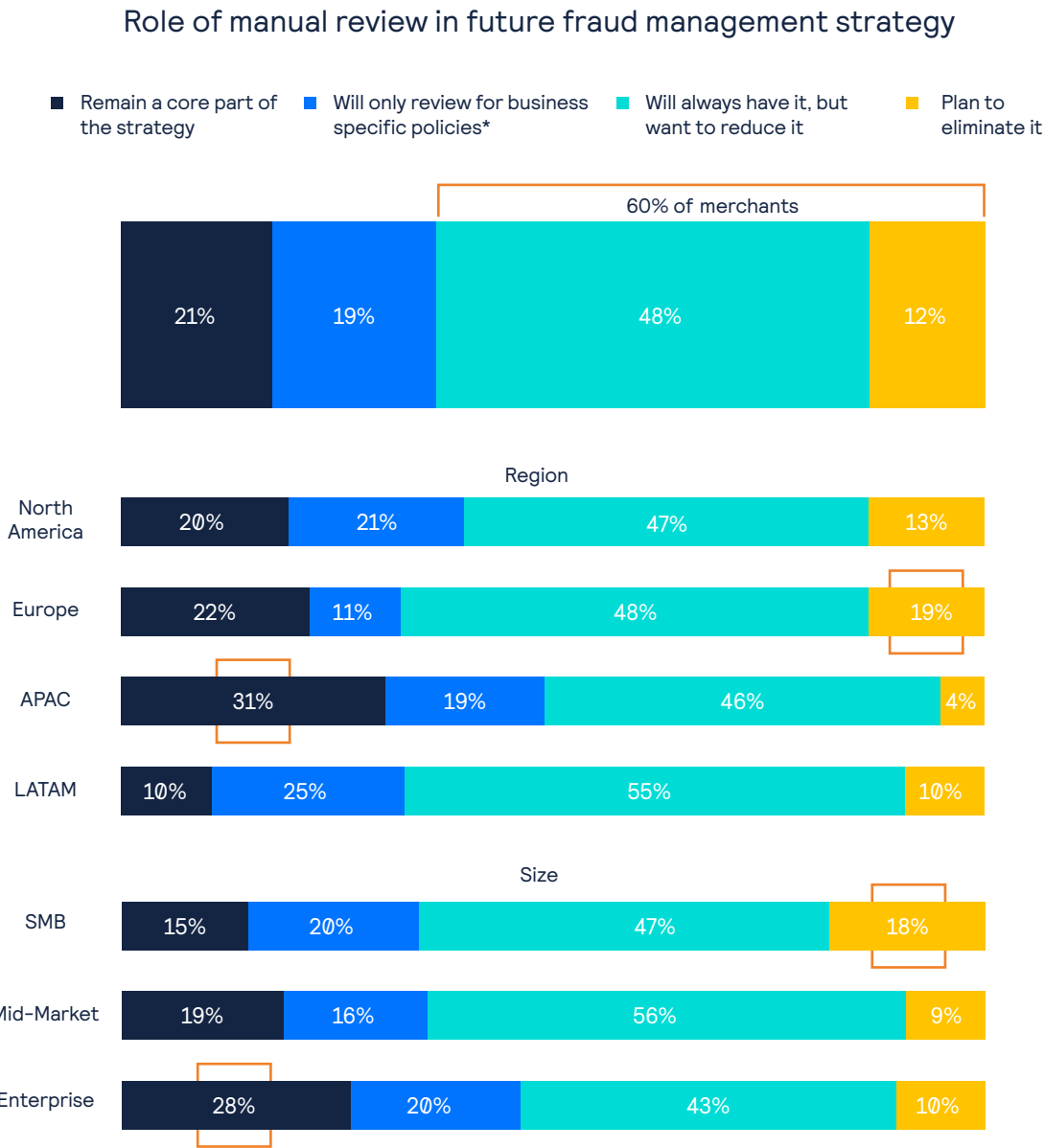


Note: Trimmed medians shown for all cost estimates.
(Parentheses show noteworthy trends compared to 2021; green text indicates an increase & red text indicates a decline)

Figure 5

Most still aiming, and more now acting, to reduce manual order review

When it comes to the role of manual order review in merchant fraud management strategies, 60% seek to reduce their reliance on this process or eliminate it entirely. European merchants and SMBs are significantly more likely to lean in this direction, with around one-in-five looking to eliminate manual review. Merchants based in APAC and at the enterprise level skew more towards retaining it as a core part of their fraud management strategy (see Figure 6).



(*policies include the likes of 1 PS5 per customer, only ship to certain countries, etc.)

Figure 6

There is some indication merchants are acting on their aim to reduce manual review, given that the share of orders manually screened and the share of screened orders that were subsequently declined due to suspicion of fraud, both decreased across all region and size segments over the past year (see Figure 7).

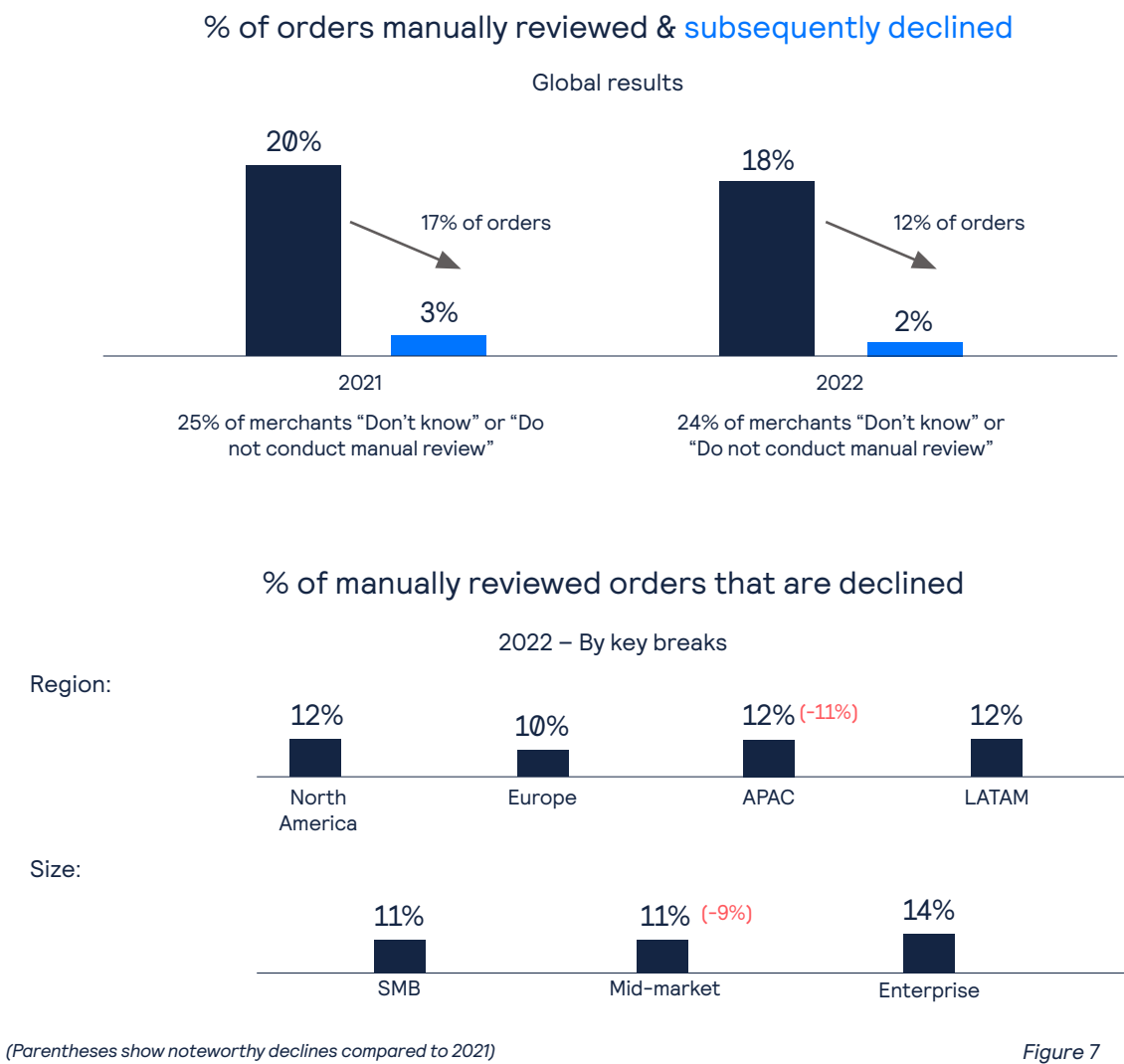
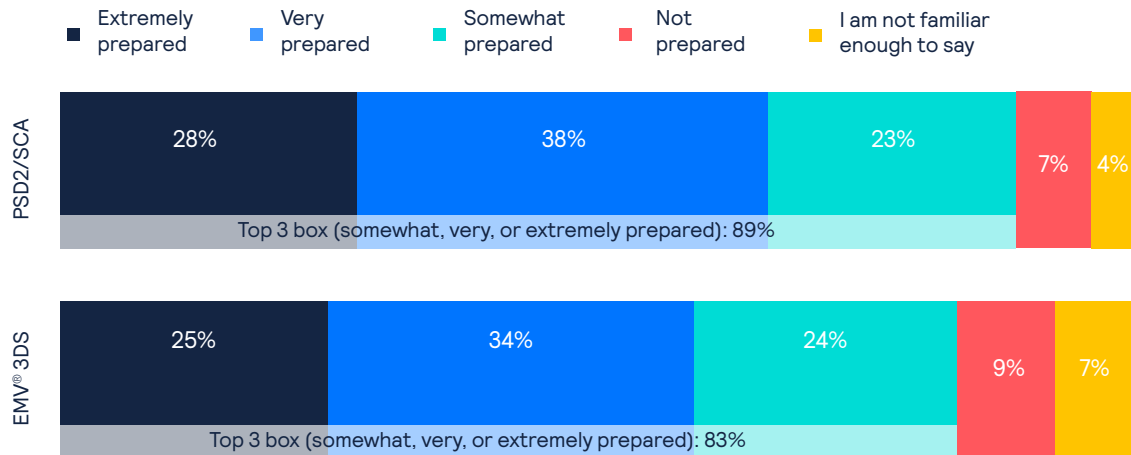


Figure 7

Most well-prepared for PSD2 SCA and EMV® 3DS to support Strong Customer Authentication

Merchants are well-prepared to support the Second Payment Services Directive (PSD2) compliance and technical requirements for Strong Customer Authentication (SCA), as well as industrywide implementation of EMV® 3DS. Around 6 in 10 feel “very” or “extremely” prepared for both, versus 1 in 10 saying their organization is “not prepared” (see Figure 8).

Merchant preparedness for PSD2 SCA & EMV® 3DS



2022 – by key breaks

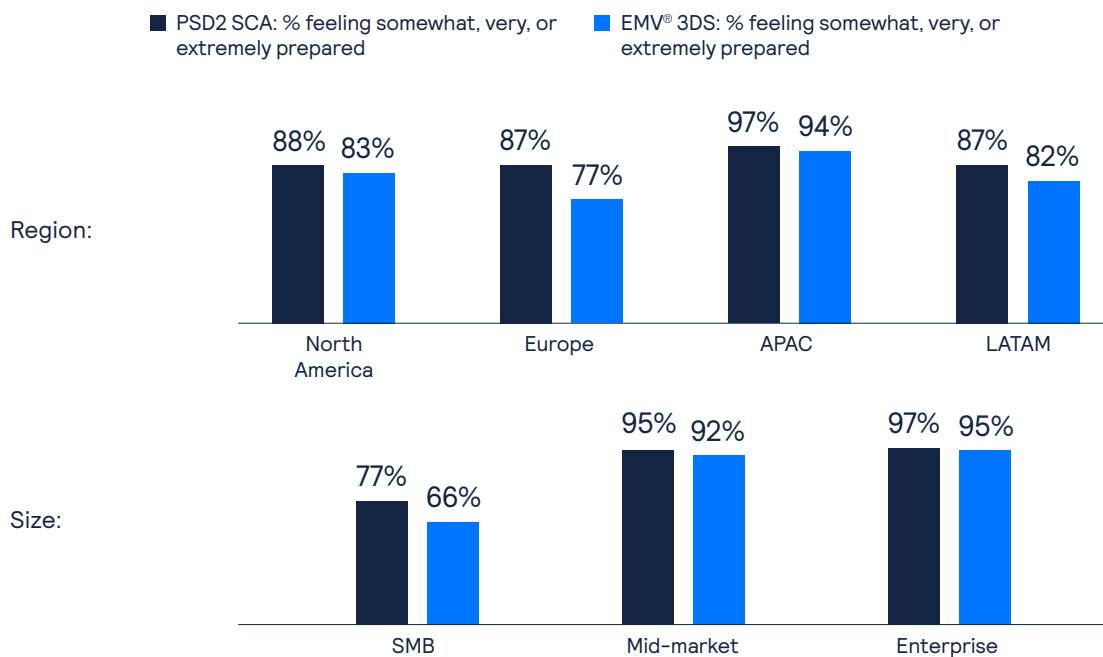


Figure 8

The consensus around preparedness for the enforcement of PSD2 SCA and/or the implementation of EMV® 3DS is encouraging. Most merchants globally expect the directive and/or the Three-Domain Secure messaging protocol to have a major impact on their organization. This is especially the case for merchants based in the APAC and LATAM regions, for mid-market and enterprise merchants.

2. Range of fraud attacks: key findings



This section of the report focuses on the types of fraud attacks eCommerce merchants are experiencing, globally and within specific regions and size segments. In addition, this section discusses the top fraud-related challenges merchants are struggling to overcome and how they have shifted and evolved since the publication of the 2021 report.

Top Fraud Attacks Remain Consistent

The four most prevalent forms of fraud faced by merchants remained consistent over the past year, as did their general incidence rates, in terms of the proportions of merchants who reported experiencing each of them. These top four fraud attacks are phishing / pharming / whaling, card testing, identity theft, and first-party misuse (also known as “friendly fraud”), and they all continue to impact around one-third of merchants, globally. That these fraud attacks aren’t experienced in isolation and are generally interrelated is a likely cause behind the prevalence of these most common attacks. Out of the top four, only first-party misuse has seen a slight decline in reported incidence, as it impacted 32% of merchants in this year’s survey, compared to 39% in 2021 (see Figure 9).



Figure 9

The top attacks reported by region and size also remained largely consistent with those in 2021, (as illustrated in figure 10, below), although there were significant shifts in incidence rates among certain segments. For instance, while card testing and first-party misuse are still the two most common fraud attacks reported by merchants in North America, the share of merchants citing each of these declined significantly. The same is true of incidence rates for loyalty fraud and coupon / discount / refund abuse among APAC merchants and of those for first-party misuse in the LATAM region. On the other hand, incidence rates for the top three attacks rose significantly among merchants based in Europe, as did the rate for identity theft in LATAM (see Figure 10).



Figure 10

First-party misuse represents sizable share of fraud attacks

First-party misuse, also referred to as “friendly fraud” or chargeback fraud, is believed by merchants to account for a sizable share of all fraud attacks or attempts (impacting around a third of merchants, as shown in the previous section of this report). Globally, merchants believe 16% of fraudulent disputes should be attributed to first-party misuse, and merchants state that most disputed transactions are the result of cardholders aiming to obtain free goods, confusion about transaction descriptors, or card issuers incorrectly processing general cardholder disputes as fraud (likely due, in part, to incentives issuers have to resolve disputes quickly). (see Figure 11 and Figure 12)

% of disputes that should be attributed to first-party misuse



Extent to which issuers incorrectly file disputed transactions as fraud

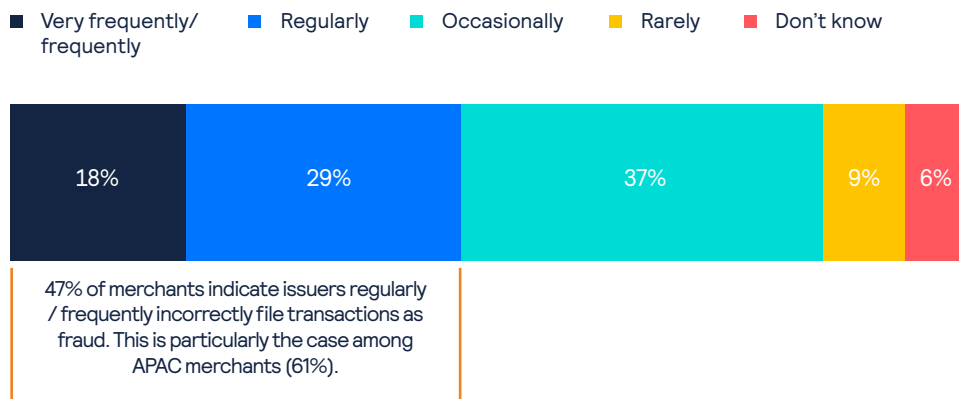


Figure 11

Common types of first-party misuse (drivers for submitting disputes)

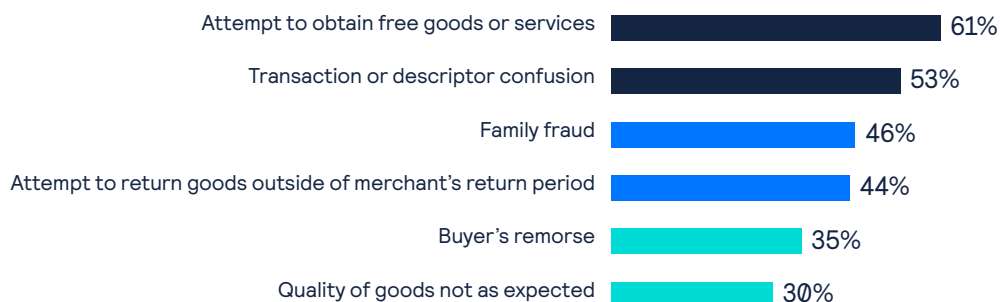


Figure 12

Key fraud challenges stay consistent in prevalence but shift in severity

Merchants must effectively prevent and mitigate fraud attacks while also grappling with a range of broader business challenges related to, and impacted by, fraud. The results of last year's fraud study illustrated both the relative incidence and severity of these fraud-related challenges, which were all tracked again in this year's survey.

The 2022 study makes clear the share of merchants facing each of these fraud-related challenges – or their respective incidence rates – has stayed remarkably consistent, year-on-year. The largest share of merchants are struggling to identify and respond to emerging fraud attacks, while also confronting the challenge of keeping up to date with payment regulations or rule changes by payment partners, and changing business models quickly due to the impact of the COVID-19 pandemic (see Figure 13).

Once again, mid-market and enterprise merchants remain far more likely to face many of these challenges, compared to SMBs.

Top fraud management challenges experienced in the past 12 months

(% = 2021 figures)

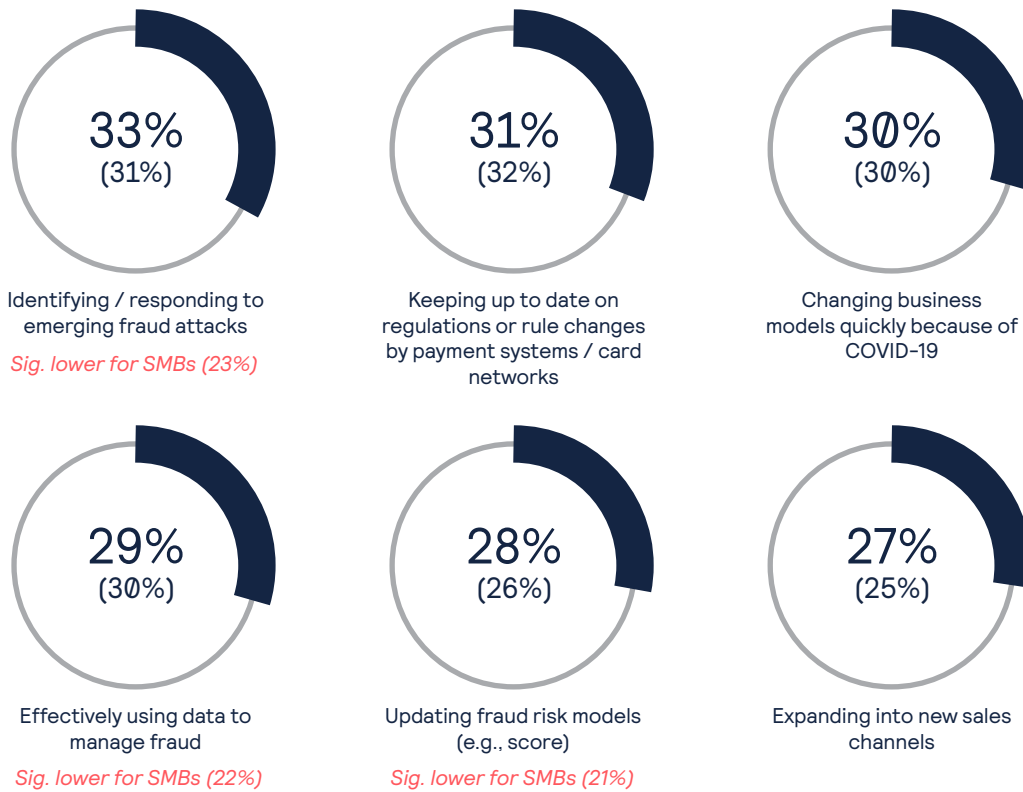
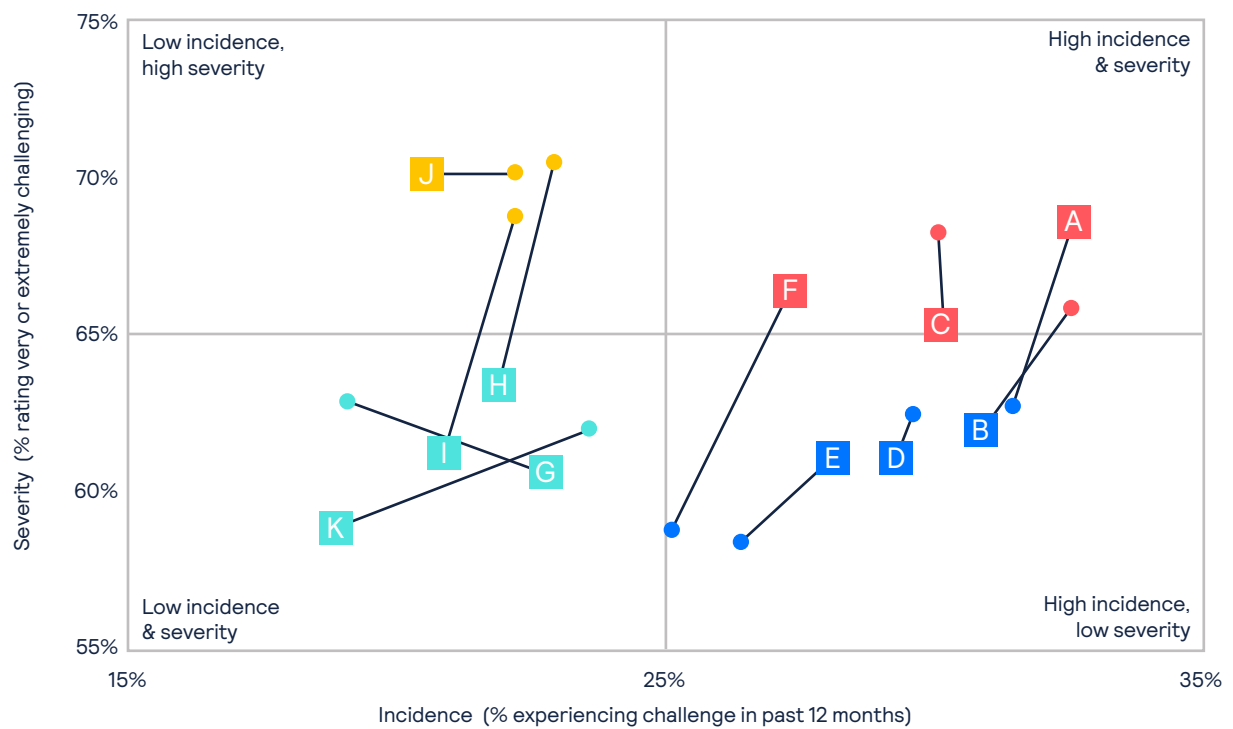


Figure 13

While the nature and prevalence of fraud-related challenges stayed fairly consistent, what did change over the past year was the relative severity or difficulty each challenge presented to the merchants facing it. Figure 14, below, indicates how both the incidence and severity of each challenge has shifted, since 2021.



Bubbles in chart show positioning for 2021

- | | |
|---|--|
| A Identifying / responding to emerging fraud attacks | G Gaps in fraud tool functionalities |
| B Keeping up to date on regulations or rule changes by payment systems | H Lack of sufficient internal resources |
| C Changing business models quickly because of COVID-19 (e.g., leading to unplanned attacks, management challenges) | I Lack of internal expertise |
| D Effectively using data to manage fraud | J Managing omnichannel fraud |
| E Updating fraud risk models (e.g., score) | K International expansion |
| F Expanding into new sales channels | |

Bolded text labels above show challenges with increasing severity

Figure 14

The challenges of identifying and responding to emerging fraud attacks, updating fraud risk models, and effectively managing fraud while expanding into new sales channels have become markedly more difficult for merchants to overcome. And while managing omnichannel fraud still has relatively low incidence compared to most other challenges, it remains an especially troublesome problem for the merchants it impacts. On the other hand, merchants are generally finding it less difficult now to overcome the challenges of staying up to date on payment regulations and payment partner rule changes, as well as managing fraud effectively despite the lack of internal resources and / or expertise, when compared to last year.

3. Fraud prevention strategies: key findings



Having discussed the impacts of eCommerce fraud on merchant businesses and the more prevalent and pernicious fraud attacks and challenges, the following section of insights examines how merchants are responding to prevent and mitigate fraud at both a strategic and tactical level.

The survey shows there has been a significant shift in the top priority driving merchants' strategic approaches to fraud management and prevention. Compared to 2021, significantly more merchants are now prioritizing "reducing fraud and chargebacks" and "minimizing fraud-related operational costs," while significantly fewer are focused primarily on "improving the customer experience (or CX)" (see Figure 15). In part, this strategic shift may be driven by rising costs and KPIs associated with eCommerce fraud (as detailed in the first section of this report). Alternatively, some merchants may have decided they've improved the customer experience sufficiently over the past year and can now focus a bit more intently on reducing fraud and chargebacks or reducing fraud-related costs, instead.

Most important fraud management priorities

(% merchants ranking each as #1 priority)

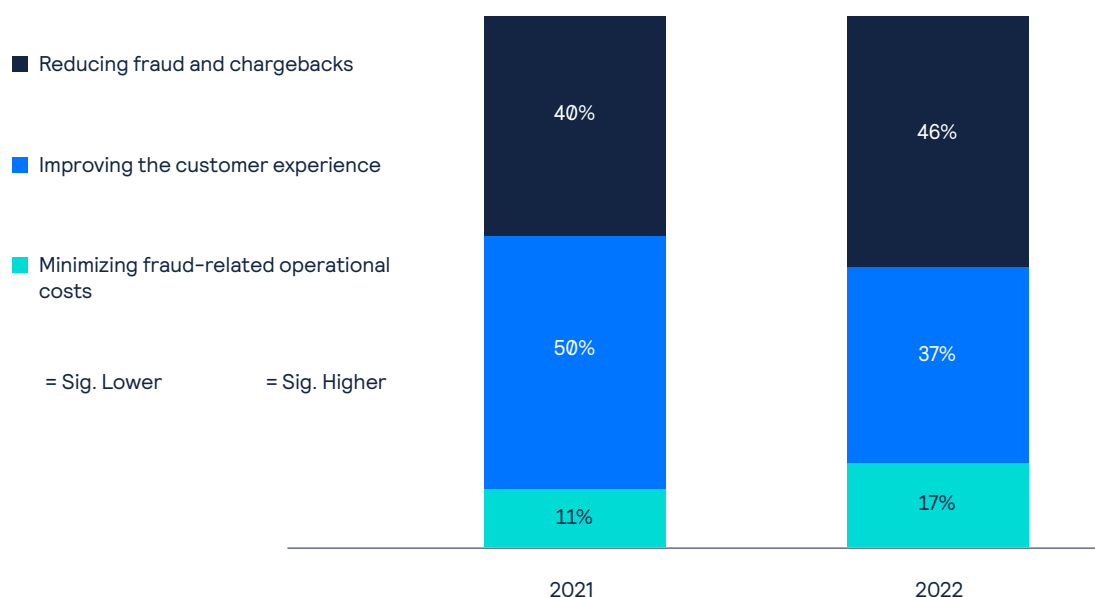


Figure 15

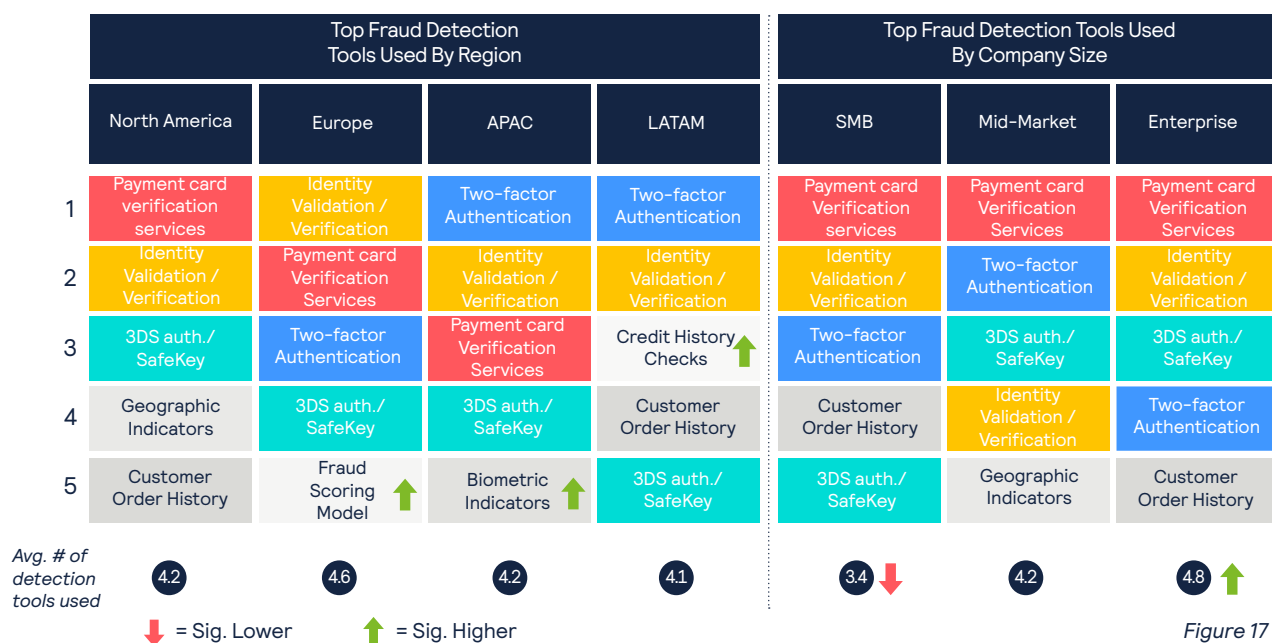
Most use multiple fraud prevention tools now and plan to add more

Digging into the tools used by merchants for fraud prevention, they currently use an average of four different tools and services to detect and thwart fraud attacks. Credit card and identity verification services, along with EMV® 3DS and two-factor phone authentication, are the most widely used anti-fraud tools, each employed by around 35–40% of merchants, globally (see Figure 16). These, and other commonly used tools, such as geographic indicators and customer order histories, are also the tools most likely to be adopted by more merchants in the future.



Figure 16

As in previous years, enterprise merchants continue to use a significantly larger array of fraud prevention tools than SMBs, and while the usage of tools has remained largely consistent, some specific tools are increasingly adopted in certain markets (see Figure 17).



Increasing correlation between tool usage and effectiveness

In contrast to the trend reflected by the 2021 survey, many of the most widely used tools today are also considered the most effective at detecting and preventing fraud. These include payment card and identify verification services, two-factor authentication and EMV® 3DS authentication, customer order histories, geographic indicators, list management and device-based results (see Figure 18). There is room for merchants to improve their fraud prevention toolkits by adopting less widely used, but highly effective, tools and techniques – most notably, company-specific fraud scoring models, biometric indicators, and multi-merchant / order velocity monitoring (see Figure 18).

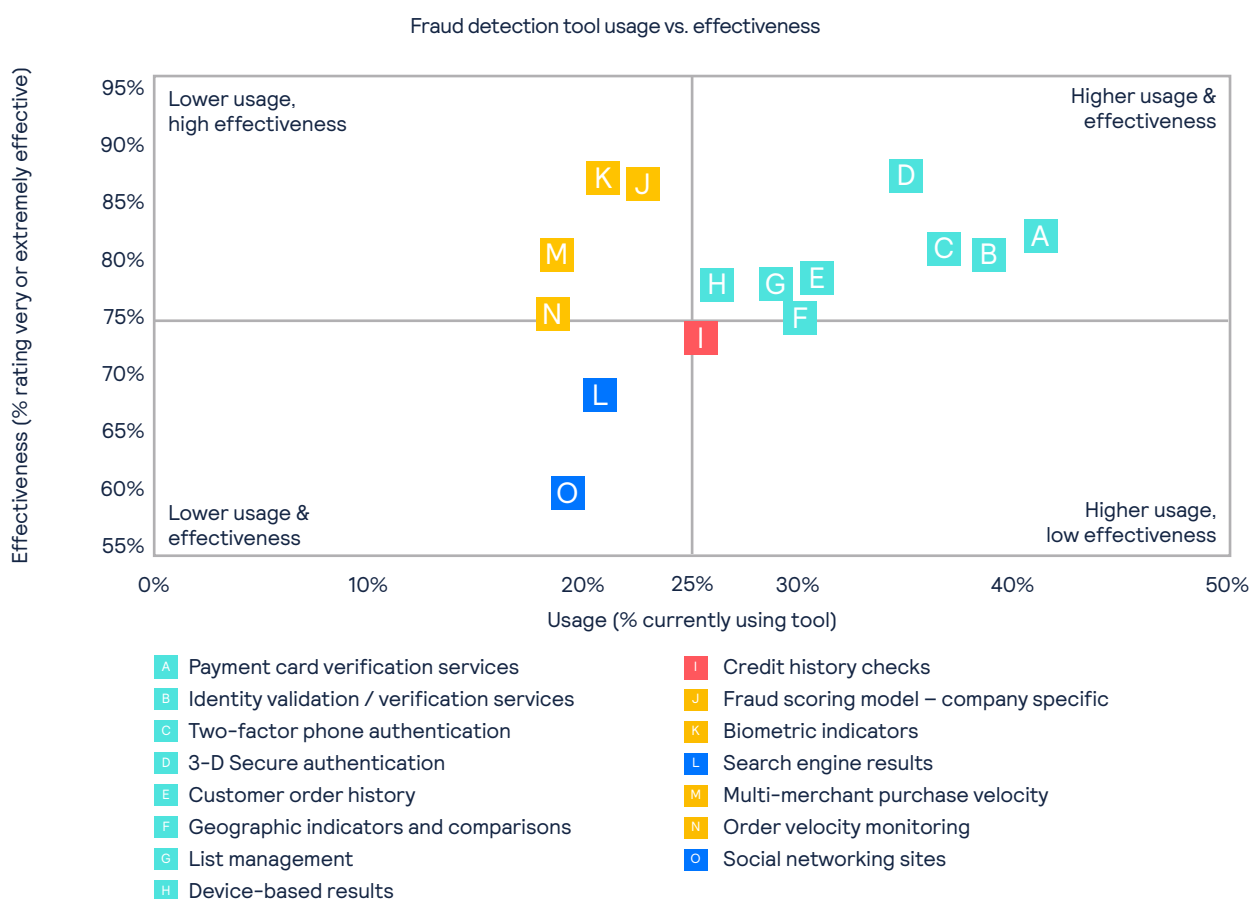


Figure 18

4. Payment acceptance and partners: key findings



In these final two sections, 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, and size.

Four main payment methods accepted and preferred, with digital and mobile payments increasingly accepted

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). Beyond these primary methods, cash is accepted by 45% 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 more likely to add digital wallets and mCommerce mobile payments to their payment acceptance portfolio than any other methods (see Figure 19).

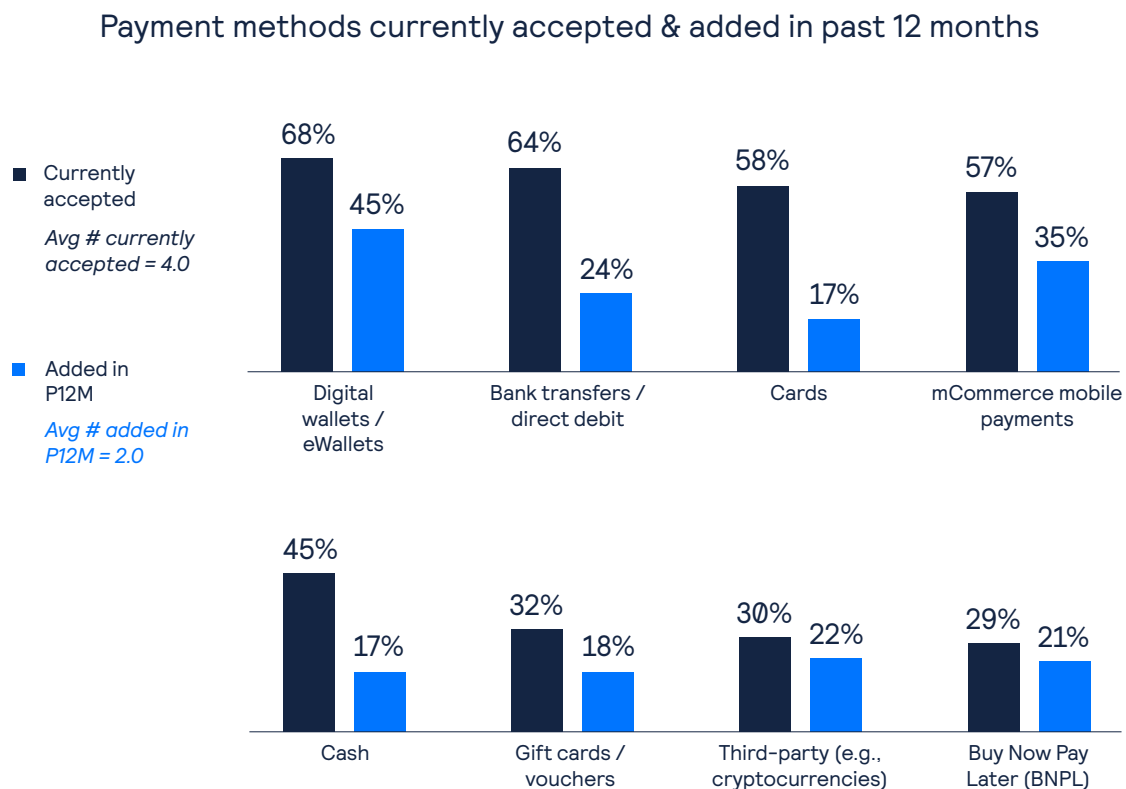


Figure 19

A closer look at Figure 19 points to some interesting trends regarding the fastest growing payment methods among eCommerce merchants globally. Third-party payments (e.g., cryptocurrency), BNPL, digital wallets, and mCommerce are being more readily adopted by merchants, with the majority of businesses currently accepting these methods adding each of them within the past year.

While there are few differences across merchant segments based on the average number of payment methods currently accepted, APAC-based merchants, mid-market and enterprise sized merchants have been more active over the past 12 months expanding the number of payment methods offered to customers (see Figure 20).

Payment methods currently accepted & added in past 12 months

	Global (NET)	Region - 2022				Size - 2022		
		North America	Europe	APAC	LAT AM	SMB	Mid-market	Enterprise
Average number currently accepted	4.0	3.7	3.9	3.9	3.8	3.7	3.9	3.9
Average number added within the past 12 months	2.0	2.0	1.7	2.6 	2.0	1.5	2.2 	2.4 

 = Sig. Higher

Figure 20

Merchants are adopting a multifaceted approach to adding new payment methods, driven primarily by the following factors:

- 01

A focus on improving customer experience
(factor for 57% of merchants)
- 02

Reaching new customer segments
(factor for 42% of merchants)
- 03

Providing access to new markets
(factor for 40% of merchants)
- 04

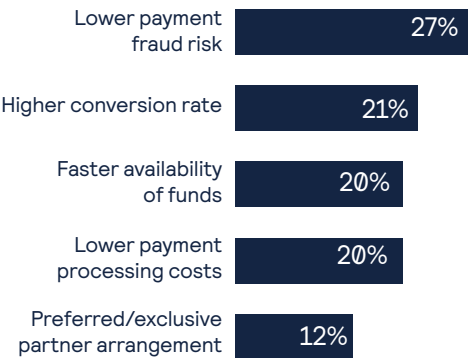
A desire to accept mobile payment methods
(factor for 38% of merchants).

In other words, merchants are continually adjusting payment acceptance offerings to better satisfy current customers, as well as to better target and attract new ones.

At the same time, nearly 9 in 10 merchants encourage customers to pay via the merchant’s preferred methods (although SMBs are significantly less likely to do so, with 75% pushing preferred methods), which yield maximum benefits in terms of the efficiency and profitability of payment operations. The top reasons for encouraging payments via merchant-preferred methods include lowering fraud risk, maximizing conversion rates, expediting availability of funds and minimizing processing costs (see Figure 21).

Merchants leverage several techniques to encourage customers to pay via preferred methods, including promoting these methods during the checkout process, offering or pre-selecting preferred payment methods prior to the main payment selection page, and providing incentives for customers to select preferred methods. (see Figure 21).

Most important reasons for encouraging use of preferred methods



Usage of approaches to encourage use of preferred methods

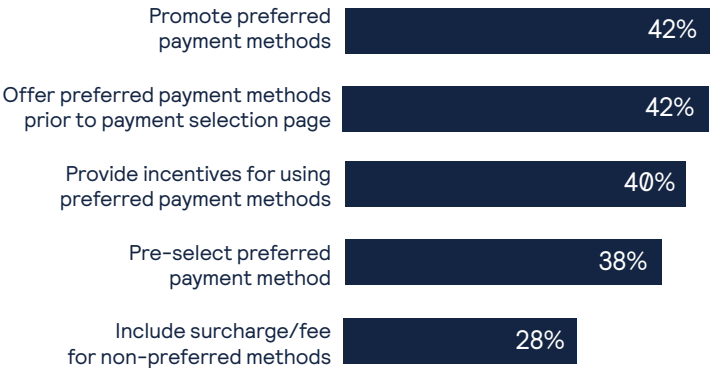
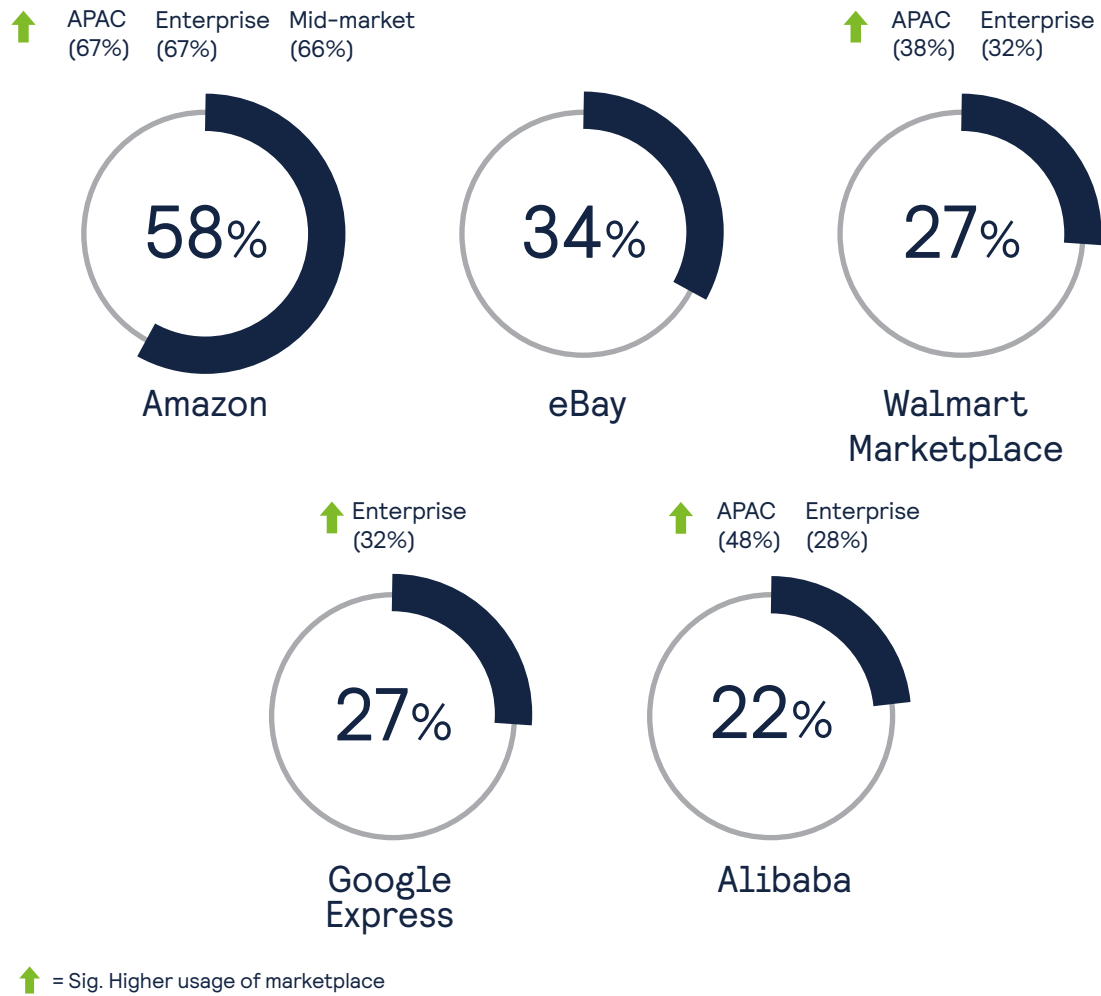


Figure 21

Customer-centric and competitive motivations also drive around 8 in 10 merchants to sell goods on third-party marketplaces (although marketplace usage is less common among SMB merchants with 64% using marketplaces). Amazon is used by the majority, while around one-third leverage eBay and nearly 3 in 10 merchants sell on Walmart Marketplace and Google Express (see Figure 22). Around 1 in 5 merchants (22%) sell on Alibaba, although it should be noted that the plurality (41%) of merchants in our survey are based in North America, versus 17% from the APAC region.

Top 5 third-party marketplaces used by merchants



Reasons for using third-party marketplaces

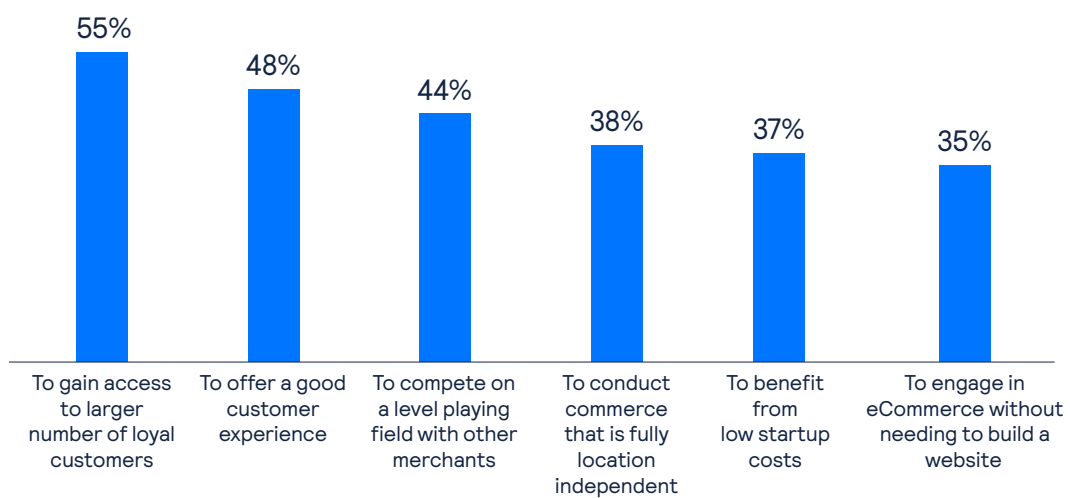


Figure 22

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 that are far more essential to supporting payment acceptance offerings: specifically, payment processors and acquiring banks.

On average, merchants leverage four payment processor connections and three different acquiring banks to support omnichannel payments, although these figures skew higher for APAC and LATAM-based merchants, as well as those in the mid-market and enterprise-size segments. Maximizing flexibility, geographic coverage, uptime, and authorizations represent the main motivators for merchants utilizing multiple acquirers, with LATAM and APAC-based merchants, and enterprise sized merchants citing a broader range of motivators (see Figure 23).

Usage of payment partners (trimmed averages shown for figures in this table)

	Global (NET)	Region - 2022				Size - 2022		
		North America	Europe	APAC	LATAM	SMB	Mid-market	Enterprise
# Of payment gateway or processor connections currently supported	4.1	4.1	3.7	4.0	4.4	3.6	4.4 ↑	4.4 ↑
# Of acquiring banks currently used	3.2	3.1	3.0	3.7 ↑	3.6 ↑	2.6	3.5 ↑	3.9 ↑

↑ = Sig. higher

Reasons for using multiple acquiring banks (among those using 2 or more acquiring banks)

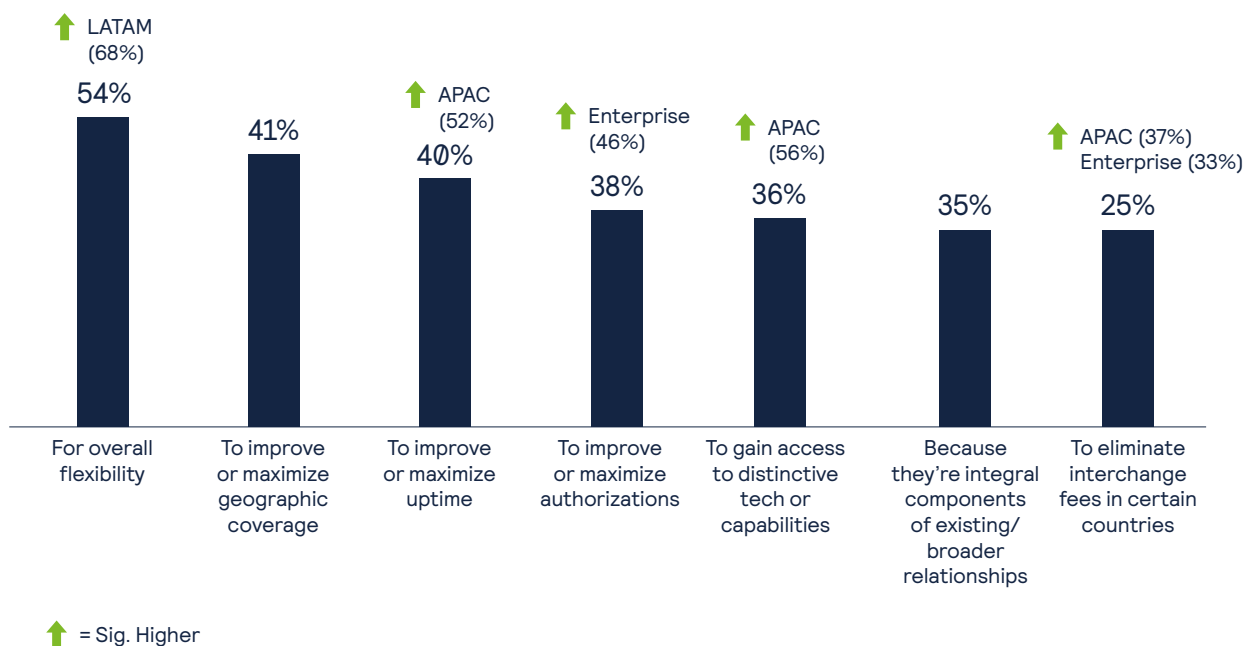


Figure 23

Payment acceptance and partnership approaches vary substantially by merchant segment

It is worth noting here that payment acceptance and partnership approaches vary significantly by merchant segment. As indicated in Figures 19–23 in this section, merchants in APAC and enterprise merchants contrast starkly with merchants in Europe and SMBs when it comes to payment acceptance methods and partners. The former are adding more new methods, using more third-party marketplaces, and leveraging more processor partnerships to support their eCommerce payments, and they cite a wider and larger range of motivations for doing all the above when compared to the latter. Time and further research will tell whether these differences in payment approaches persist and widen across merchant segments, or whether merchant payment acceptance strategies and partnerships become more globally uniform in the future.

5. Payment management: key findings



This final area of insights shows what merchants are doing to optimize the customer payment experience, as well as internal payment management processes and operations. Here, the survey data once again reveal clear and significant divergences in the payment management approaches employed by merchants in different segments.

Merchants experimenting with, but not widely adopting, new payment experiences

Merchants are rolling out a diverse range of novel retail approaches and customer experiences to better serve customers and facilitate payments, but these have yet to be widely adopted. The top retail approaches, each used by over 3 in 10 merchants globally, include reserve online, purchase in store; buy online pickup in store; phone orders; and buy online and ship to store. The top customer experiences, used by over a third of merchants globally, are chatbots / customer service AIs and connected devices (see Figure 24). APAC, LATAM, mid-market, and enterprise merchants are more likely to be early adopters of these new approaches and experiences, over-indexing on implementation for several of the approaches and experiences listed below.

Usage of retail approaches

Avg. # of retail approaches used: 3.4



Customer experiences offered

Average # of customer experiences offered: 2.6

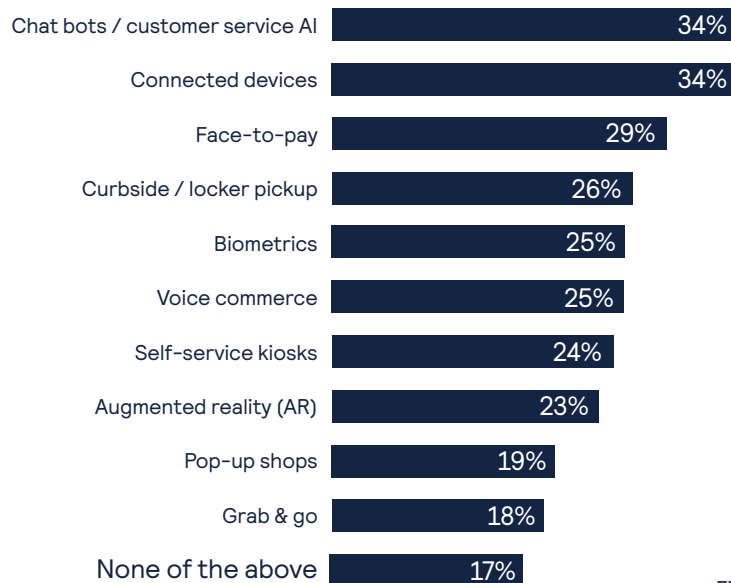


Figure 24

Most monitor three to four key indicators tied to payment management

Most merchants focus on 3 to 4 key performance indicators for payment management. Payment success rate, revenue, and cost of payments represent the top three KPIs tracked by merchants, globally, followed by authorization, authentication and loss rates (see Figure 25). Enterprise merchants monitor a significantly larger number and variety of payment management KPIs, especially compared to SMBs, which tend to focus on just the top three.

Most important KPIs for payment management

Average # of KPIs tracked: 3.7



Enterprise (4.2 KPIs tracked)



SMB (3.2 KPIs tracked)

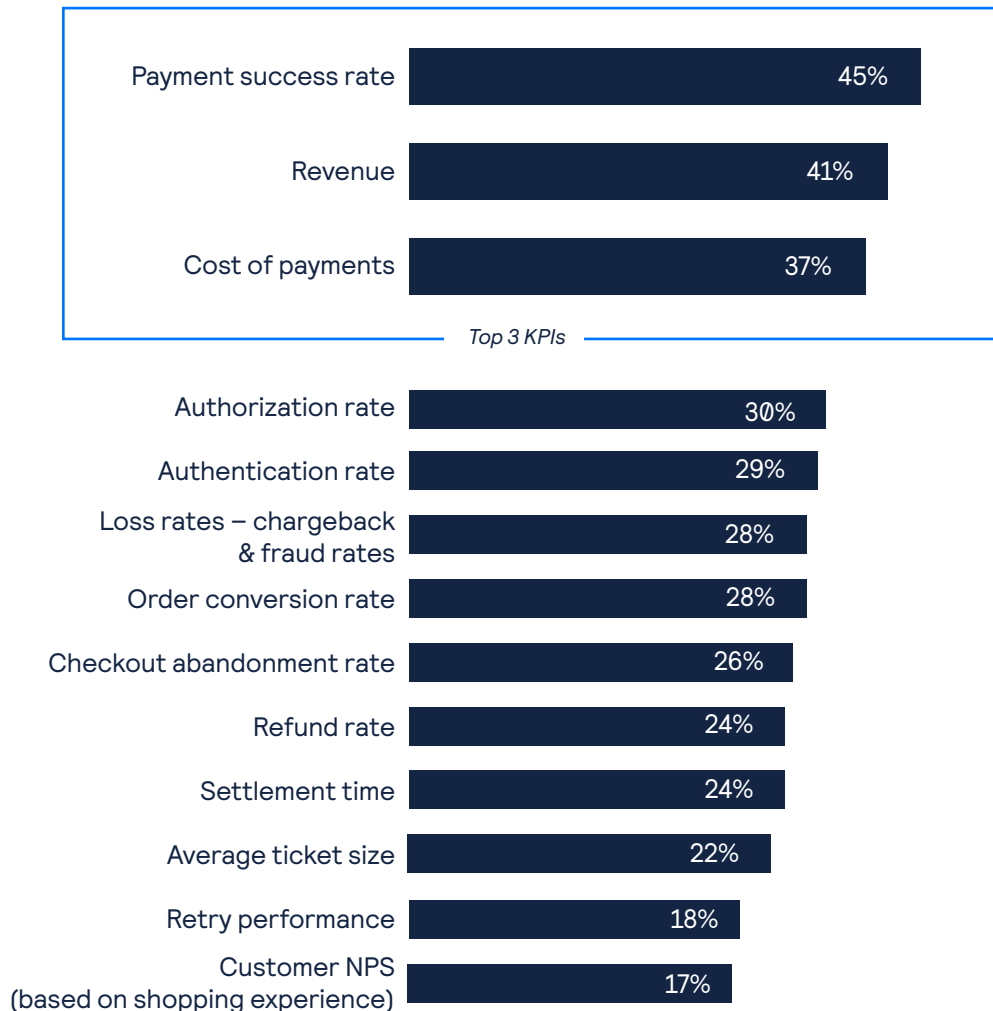


Figure 25

Multiple techniques used To maximize authorization rates

While authorization rates are a key indicator tracked by only 3 in 10 merchants, the vast majority (86%) employ multiple techniques aimed at maximizing authorizations when processing payment transactions. 3DS2, intelligent routing, machine learning, and automated retries are the most widely used techniques, although sizable shares also leverage account updaters, tokenization, and dynamic currency conversion as well (see Figure 26).

The majority of merchants that employ these techniques support them with the use of third-party data sources.

Techniques used to maximize authorization rates & % using third-party data with each

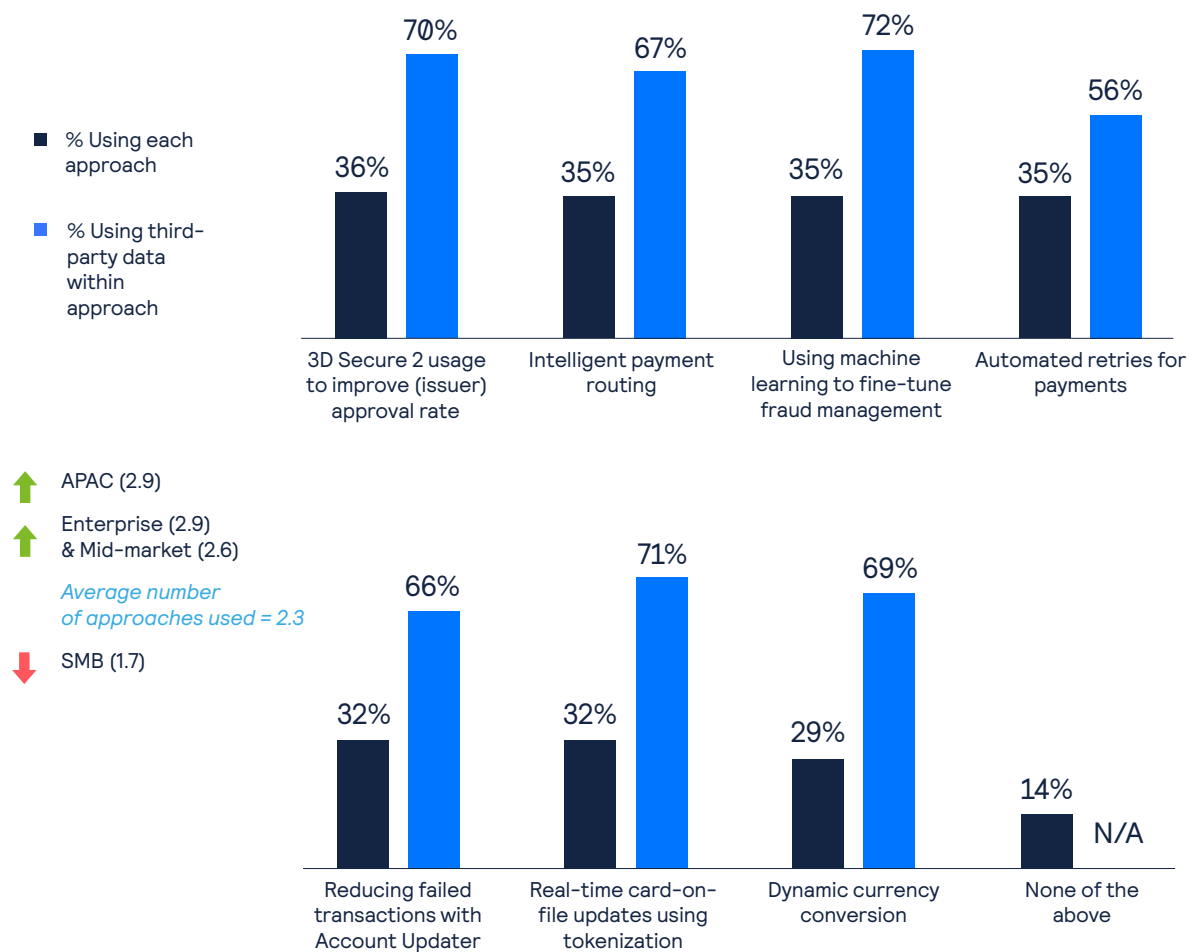


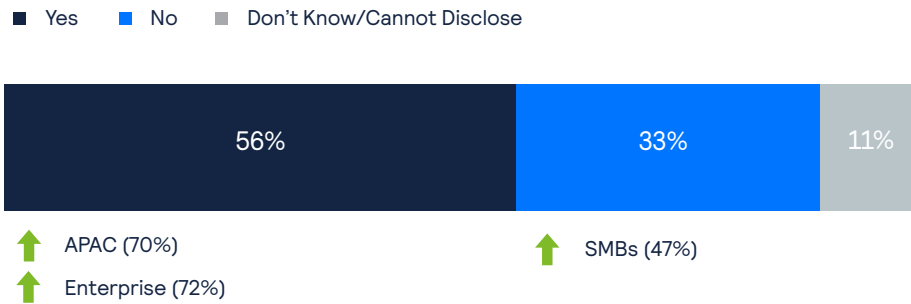
Figure 26

Majority use tokenization to enhance security, customer trust and authorization rates

Lastly, turning to the use of tokenization in payment management (meaning the encryption of customer card numbers, either in the merchant's own internal databases, or via the merchant's card network / card issuer / wallet provider payment partners), the majority of merchants currently utilize tokenization, with enterprises and APAC-based merchants over-indexing significantly in this area. SMBs, meanwhile, are much more evenly split, as nearly half (47%) have yet to implement tokenization (see Figure 27).

The most common motivation for employing tokenization is to improve payment security and reduce risk – i.e., protecting customer privacy and reducing the risk of data breaches. Fostering trust among customers, improving authorization rates, optimizing the customer experience, and ensuring robust compliance with Payment Card Industry (PCI) Data Security Standards (DSS) and payment regulations are also important rationales for merchants leveraging tokenization.

Usage of tokenization in payment management



Reasons for using tokenization

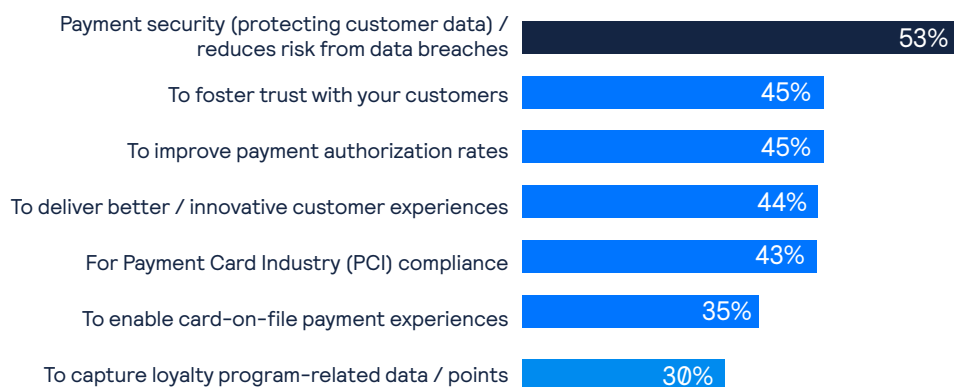


Figure 27

Conclusion

Overall, the results of this survey illustrate how eCommerce merchants have been making substantial progress in advancing their approaches to managing fraud and payments. This is particularly impressive given how critical, complex, and challenging the issue of global eCommerce payment fraud is for merchants.

This report highlights several encouraging trends and indicators that together send a positive signal about merchants' collective capabilities to successfully improve and advance fraud management strategies to better protect business and customers. This report also highlights several ways merchants have considered their approach to better serve customers by expanding channels to enable purchases, while still ensuring safety is at the forefront of these decisions.

Enterprises and APAC-based merchants are leading the way in many of these areas, relative to merchants in other regions and size segments. However, as the insights and analysis above make clear, there is opportunity for merchants of all sizes and in all regions to learn from their peers and monitor trends, and there is still ample room for merchants of all sizes to further advance and improve to prevent and mitigate fraud and to optimize and enhance payments and the customer shopping experience in 2022 and beyond.

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 enables businesses to operate with agility and reach their digital commerce goals by enhancing customer experience, helping grow revenues and mitigate 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



As an independent, not-for-profit business association, the Merchant Risk Council's mission is to facilitate collaboration between eCommerce payments and risk professionals. Year-round, the MRC provides valuable resources to its members that include proprietary educational content, webinars, best practices, industry trends, benchmarking reports and whitepapers. In addition, the MRC hosts four annual conferences in the US and Europe as well as several regional networking events which provide an opportunity for industry professionals to build stronger connections with industry stakeholders.

For more information, please visit: merchantriskcouncil.org



Since 2005, Verifi has been a leader in the payments industry, providing innovative, end-to-end payment solutions that protect against fraud, prevent and resolve disputes, and recover revenue lost to chargebacks. In 2019, Verifi was acquired by Visa, combining technologies to provide enhanced fraud and dispute management solutions on a global scale. Verifi creates strategic, adaptive technologies for sellers, payment facilitators, acquirers, and issuers, building sustaining partnerships to deliver value, increase profits, and promote brand growth.

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, digital wallet and mCommerce mobile payments have the highest average conversion rates, with means ranging from 30 to 40 percent. Conversion rates are significantly higher for mobile payments accepted by merchants in North America (see Figure 28).

Average conversion rate by payment method (median/ <i>mean</i>)	Overall	North America	Europe	APAC	LATAM	SMB	Mid-Market	Enterprise
Cards	30% 39.5%	30% 43.5%	35% 41.9%	20% 30.3%	30% 36.0%	40% 43.7%	29% 33.8%	30% 38.4%
Bank transfers / direct debit	25% 33.9%	30% 40.7%	25% 36.4%	20% 28.8%	20% 23.3%	25% 37.1%	25% 31.4%	25% 31.8%
Digital wallets / eWallets	25% 33.6%	30% 39.2%	20% 30.9%	25% 32.5%	18% 22.5%	30% 37.1%	25% 30.6%	25% 33.0%
mCommerce mobile payments	25% 30.0%	30% 39.2% 	20% 24.8%	20% 25.8%	15% 18.1%	25% 32.9%	20% 26.2%	25% 30.2%
Buy Now Pay Later	20% 27.7%	30% 32.9%	20% 19.7%	20% 24.0%	15% 20.3%	25% 31.1%	20% 25.0%	20% 27.3%
Third-party payments	20% 25.4%	25% 33.2%	15% 16.5%	17% 21.1%	17% 16.8%	20% 28.5%	20% 23.3%	20% 24.4%
Gift cards / vouchers	15% 24.9%	20% 26.6%	15% 29.7%	20% 25.1%	10% 14.2%	10% 26.9%	20% 22.3%	18% 24.9%

(All means calculated with trimmed averages)  = Sig. Higher

Figure 28

When it comes to payment acceptance, the same four methods (cards, debit transfers, digital wallets and mobile payments) again boast the highest average rates, with means ranging from 45 to 55 percent, globally (see Figure 29).

Average acceptance rate by payment method (median/ <i>mean</i>)	Overall	North America	Europe	APAC	LATAM	SMB	Mid-Market	Enterprise
Cards	50% 54.3%	60% 56.9%	60% 59.2%	30% 45.6%	50% 48.4%	60% 59.3%	45% 50.1%	40% 50.8%
Bank transfers / direct debit	35% 50.1%	55% 57.1%	70% 56.6%	25% 43.0%	20% 34.5%	60% 56.9%	30% 45.9%	29% 44.4%
Digital wallets / eWallets	40% 48.0%	50% 53.0%	50% 53.8%	30% 41.7%	25% 33.3%	50% 53.8%	30% 45.7%	35% 44.6%
mCommerce mobile payments	30% 44.3%	40% 50.2%	32% 50.4%	25% 36.2%	20% 29.0%	40% 50.4%	30% 40.1%	30% 41.9%
Buy Now Pay Later	30% 37.8%	30% 41.3%	25% 40.7%	20% 27.3%	20% 30.8%	35% 46.7%	29% 33.1%	25% 35.2%
Gift cards / vouchers	20% 36.2%	20% 37.8%	25% 49.9%	20% 31.2%	10% 19.3%	20% 39.7%	20% 33.5%	20% 35.9%
Third-party payments	25% 36.1%	32% 43.5%	20% 34.9%	20% 28.4%	15% 21.9%	25% 41.2%	23% 30.4%	21% 35.9%

(All means calculated with trimmed averages)

Figure 29

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?*

Figure 4:

- *Please indicate the percent of your annual eCommerce revenue lost due to payment fraud globally, i.e., fraud rate by revenue.*
- *Please indicate the percent of your annual eCommerce revenue lost due to payment fraud on orders from your country, i.e., domestic orders).*
- *Please indicate your order rejection rate for your country, i.e., domestic orders*
- *Please indicate your order rejection rate for outside your country, i.e., international orders.*
- *Please indicate the percent of accepted annual eCommerce orders that turned out to be fraudulent (i.e., fraud rate by order) from your 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 your country, i.e., international orders.*
- *Please indicate the percent of eCommerce orders for which you have received chargebacks due to fraud.*

Figure 5: *Please indicate the percent of your annual eCommerce revenue your organization spends to manage payment fraud — excluding actual fraud losses.*

Figure 6: *How do your organization's future fraud strategy plans incorporate manual review?*

Figure 7:

- *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 8:

- *How prepared would you say your organization is for PSD2, in particular, strong customer authentication (SCA)?*
- *And, how prepared would you say your organization is for EMV[®] 3DS?*

Figure 9 and Figure 10: *Which of the following types of fraud attacks, if any, have you ever experienced at your organization?*

Figure 11:

- *What percentage of (all) fraudulent disputes do you feel should be attributed to first-party misuse (i.e., friendly fraud or chargeback fraud)?*
- *To what extent do you believe disputed transactions are filed or categorized incorrectly as “fraud” by issuers (i.e., when no fraud has taken place, but the transaction is categorized as fraud)?*

Figure 12: *Which, if any, of the following reasons do you expect causes first-party misuse (i.e., friendly fraud or chargeback fraud) to occur at your company?*

Figure 13: *Which of the following challenges related to eCommerce fraud management, if any, has your organization experienced in the last 12 months?*

Figure 14:

- *Which of the following challenges related to eCommerce fraud management, if any, has your organization experienced in the last 12 months?*
- *And how challenging would you say each of the following have been for your organization to manage?*

Figure 15: *Now, which one would you say is the most important to your organization when evaluating fraud management practices?*

Figure 16 and Figure 17: • *Please indicate which tools your organization currently uses.*

Figure 18:

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

Figure 19 and Figure 20:

- *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 21:

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

Figure 22

- *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 23:

- *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 24:

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

Figure 26:

- *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 27:

- *Does your organization currently utilize tokenization as part of its payment management?*
Note: By tokenization, we mean encryption of customer card numbers, either in your own internal databases, or via your card network / card issuer / wallet provider payment partners.

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

Figure 28: *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 29: *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.*

For more information,
please visit: cybersource.com

