GLOBAL FRAUD SURVEY RESULTS 2021

In partnership with

cybersource
A Visa Solution

MRC
Building Better Commerce
Fraud & Payments Professionals

Report Contents

Overview

The Merchant Risk Council (MRC) and Cybersource are pleased to present the results of the 2021 Global Fraud Survey, an educational report that conveys transparent and unbiased research. This report is based on a survey of MRC and non-MRC merchants from around the globe, who were asked about their eCommerce fraud experience and mitigation practices.

The survey results provide the MRC merchant community with the latest industry fraud data, fraud management methods used by their peers, and a robust set of performance benchmarks that members can use to help optimize their business.

The research was conducted between March and April of 2021. Overall, the survey data shows that MRC merchants, in particular, are making good progress in minimizing the impact of eCommerce fraud.

The MRC would like to thank the participants for taking the time to complete the online survey, Cybersource for managing the research, and B2B International for directing the program and providing the analysis.

Executive Summary

The key results and findings from this year's survey are organized into three focus areas within this report, each covering a central question integral to understanding the state of eCommerce fraud and merchant fraud management.

First, the report examines the business impact of fraud to understand the effects fraud is having on merchant businesses today and how those vary across regions and size segments. Then the report delves into the range of fraud attacks merchants are experiencing to illuminate the types of fraud threats merchants are facing and where they are most vulnerable. Finally, the report explores fraud prevention strategies to understand how merchants are addressing payment fraud at both a strategic and tactical level.

Below, are the key insights from each of these areas:

Business Impacts of Fraud – *What are the effects of fraud?*

- Fraud attempts, costs, and other fraud management KPIs have increased, with merchants in APAC & Latin America, and mid-market merchants, in particular, feeling the effects of a turbulent year.
- MRC members are faring better than non-members, reporting lower fraud rates by revenue and using a wider variety of fraud prevention tools to thwart a larger variety of attacks.
- Most organizations want to reduce their dependency on manual review (either in part or entirely); a larger proportion of MRC members are likely to eliminate the use of manual review in the future.

Range of Fraud Attacks – *Where are merchants most vulnerable?*

- The variety of fraud attacks merchants experience has declined (although the volume of attacks has increased).
- Friendly fraud & card testing have surpassed phishing/pharming & identity theft as the most common attacks, globally.
- MRC Members have registered a broader range of fraud attacks than non-members (due, in part, to the more diverse range of fraud detection tools implemented by MRC members and training on the types of fraud attacks out there received by MRC members, allowing them to distinguish between the types of attacks experienced).

Fraud Prevention Strategies – *How are merchants addressing the issue?*

- Protecting and improving the customer / shopping experience has become the main strategic imperative for merchants related to fraud management practices.
- On a tactical level, merchants are rationalizing their fraud management toolkits, relying more heavily on just a handful of widely used tools (primarily CVN and email verification).
- Many of the most effective tools are not the most widely adopted by merchants. However, MRC members are more likely to be early adopters of more advanced and effective tools.

Survey Firmographics

The survey was conducted in March & April of 2021. 650 merchants involved in eCommerce fraud management decisions at their companies (including 38 MRC members) participated. The sample includes businesses based in four geographic regions, with broad representation across all size tiers, sales channels, and merchant categories. The charts below, show the breakdown of merchants across key firmographics at the overall level.

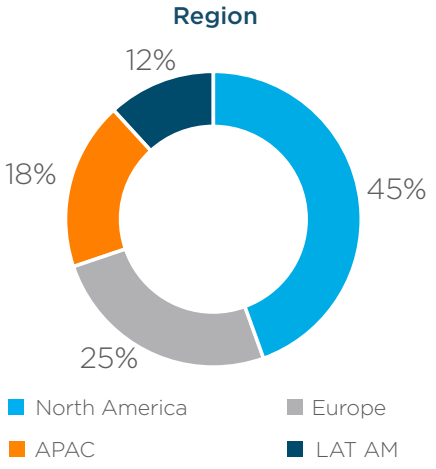


Figure 1

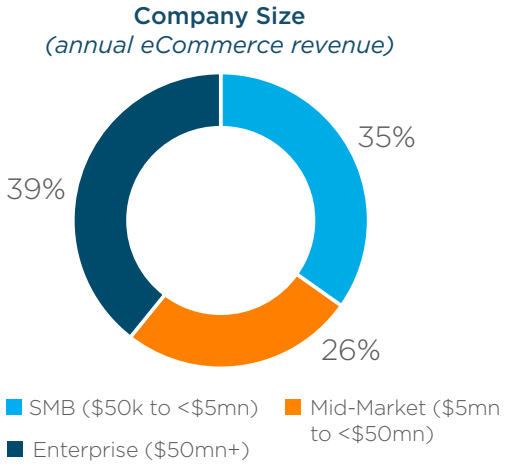


Figure 2

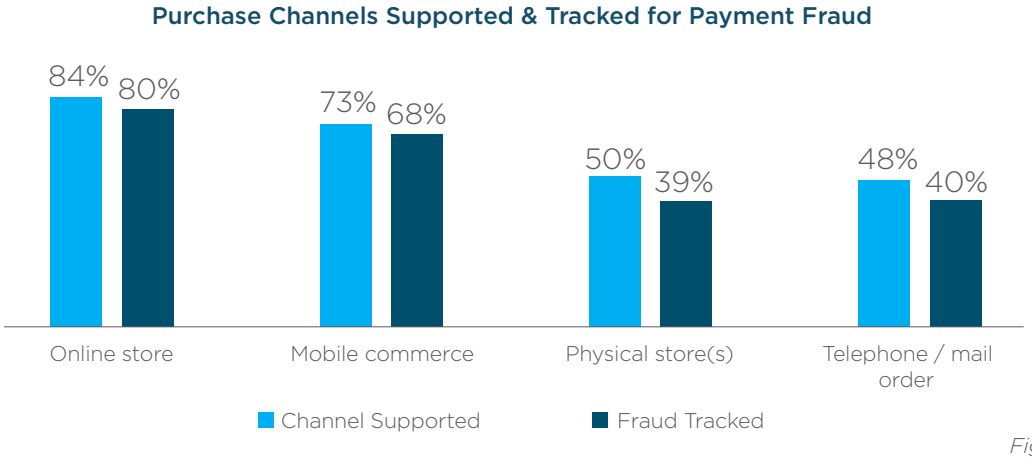


Figure 3

7 in 10 MRC members included in our sample are based in North America (26 out of 38), with the remaining members largely based in Europe (10 out of 38). Around 9-in-10 MRC members are Enterprises with $50mn+ in annual eCommerce revenue (34 out of 38).

The share of merchants in the sample who support purchases through mobile commerce and telephone / mail order channels rose significantly this year, compared to our previous study in 2019 – from 65% to 73% for mobile and from 34% to 48% for telephone / mail order. Both channels have undoubtedly become more attractive and more important to merchant businesses over the past two years, due to the restrictions on in-store commerce caused by COVID-19 and the rising internet penetration and popularity of smartphones, worldwide.

MRC members sampled this year are significantly more likely to accept purchases through online stores and mobile commerce purchase channels, than non-members. MRC members are also significantly more likely to track payment fraud through these channels, than non-members.

Business Impact of Fraud: Key Findings

The first area of insights illustrates the impact eCommerce fraud has on merchant businesses, how those impacts have changed and evolved since 2019, and where merchants have been more successful in thwarting fraud attempts and mitigating their harms to the organization.

In addition to discussing the four overall findings outlined below, in-depth insights are offered on two specific topics relevant for understanding how fraud is affecting merchant businesses: the current state of manual order review and merchant preparedness and expectations regarding the recent amendment to EU's Payment Service Providers Directive, known as PSD2.

01 COVID led to an increase in fraud attacks and fraud rate by revenue for around three-quarters of merchants; all fraud management KPIs have increased since 2019.

02 Spending on fraud management has spiked – increasing five-fold since 2019, as a share of eCommerce revenue. Mid-market merchants are spending the most of any merchant size segment.

03 COVID has driven bigger fraud impacts on organizations based outside of North America. Those based in APAC have been hit hardest, prompting an increased focus on fraud management and increased spending in this region.

04 MRC members have adapted well, registering a similar uptick in fraud attempts but reporting lower fraud rates by revenue (and other KPIs), compared to non-MRC members.

The emergence of COVID-19 and the resulting restrictions on normal, offline commerce over the past two years both catalyzed online sales and catapulted the importance of eCommerce as a critical sales channel for many merchants, worldwide. It was no surprise, then, to see that 9 out of 10 merchants now consider managing eCommerce fraud "very or extremely important" to their overall business strategy (see Figure 4). Moreover, managing eCommerce fraud has become pertinent to merchants based in the Asia-Pacific (APAC) region; the data shows the biggest increase in the share of merchants considering this issue highly important to their overall business strategy, from 82% in 2019 to 95% this year.

Importance of Ecommerce Fraud Management to Overall Business Strategy

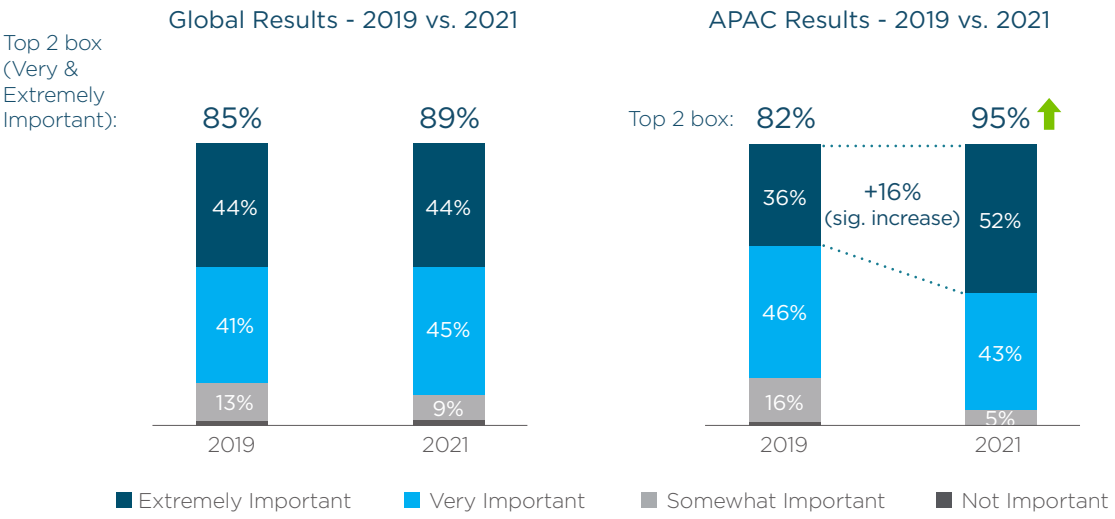


Figure 4

The importance of eCommerce fraud management has been elevated not just by rising eCommerce sales but by a global increase in fraud attempts and attacks experienced by merchant businesses. In comparison to the days before COVID, around three-quarters of merchants reported increases in both fraud attempts and fraud rates by revenue (Figure 5).

Proportion of Organizations Reporting Increases in Fraud Attempts & Fraud Rate by Revenue

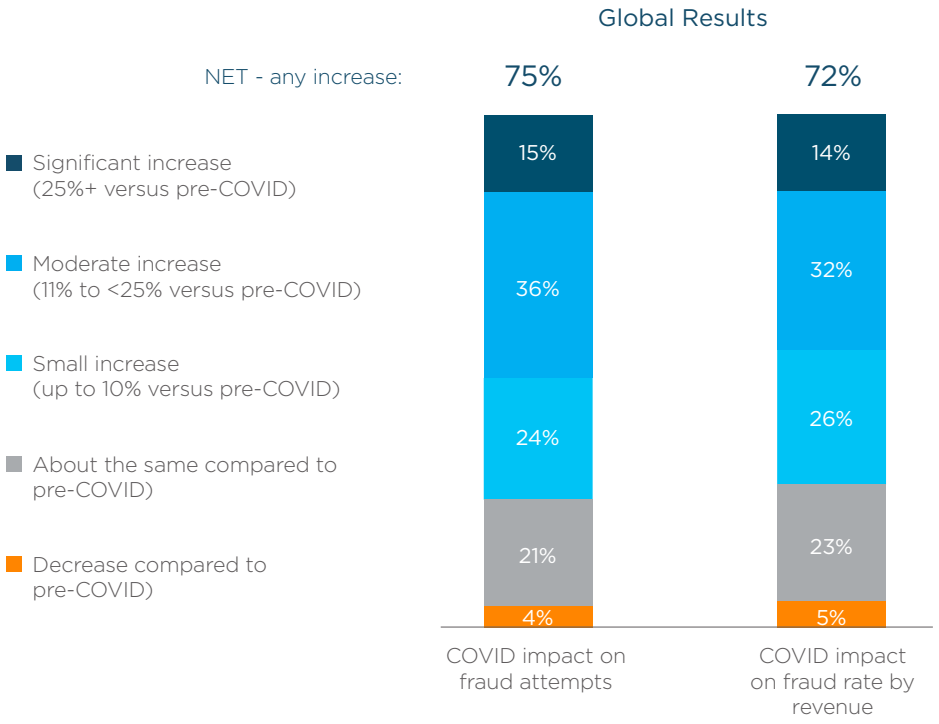


Figure 5

COVID spurred an increase in fraud attempts and fraud rates by revenue. This has been especially impactful on merchants based outside North America, mid-market, and enterprise organizations. These groups boast the biggest online revenues. Notably, even though non-MRC members experienced similar fraud attempts, MRC members are faring significantly better, in terms of preventing those attempts from driving similar increases in lost revenue (Figure 6).

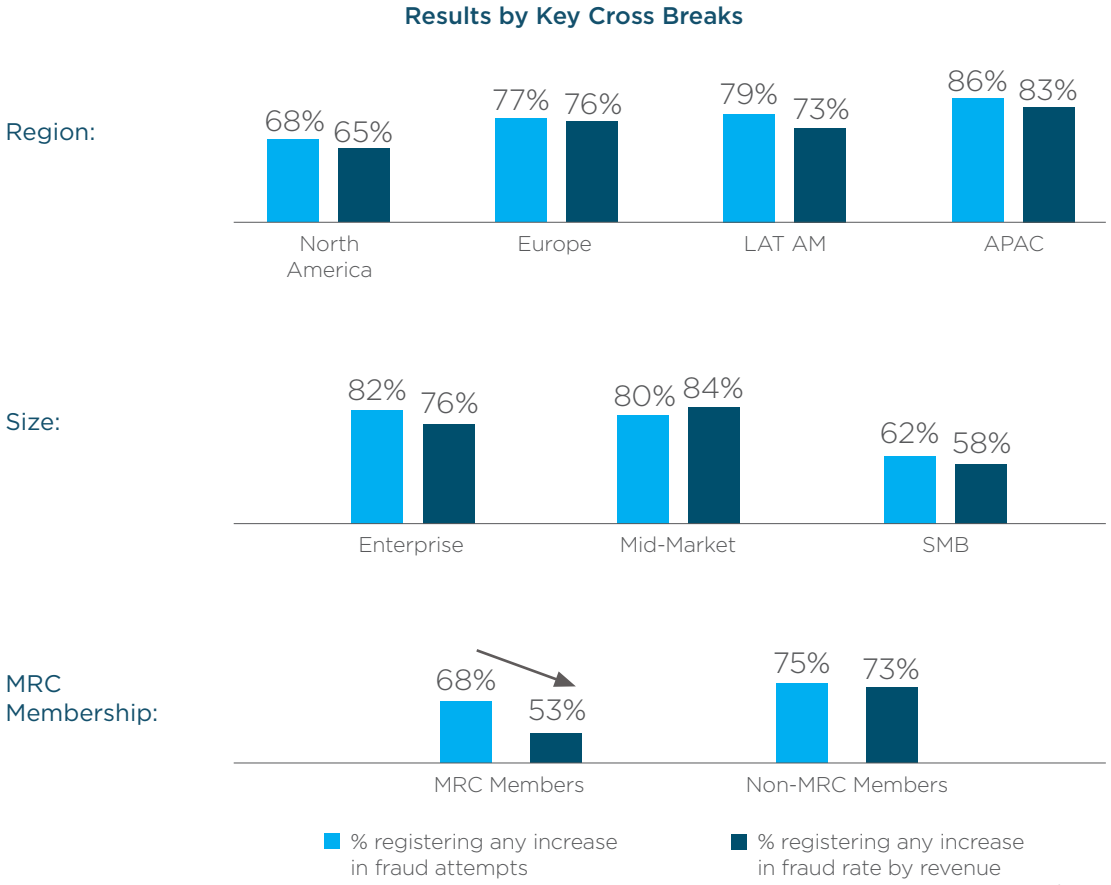
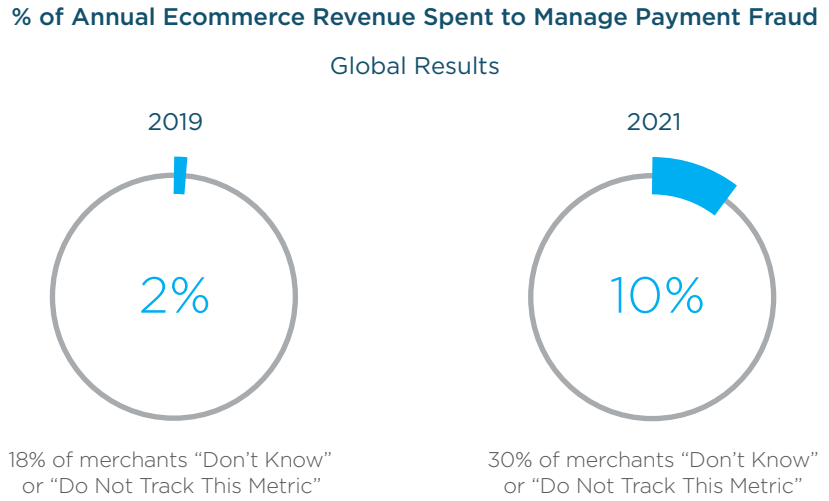


Figure 6

As fraud attempts and fraud rates by revenue have risen, fraud management costs have increased five-fold, on average, compared to pre-COVID, from an average of 2% of annual eCommerce revenue in 2019 to around 10% this year (Figure 7).

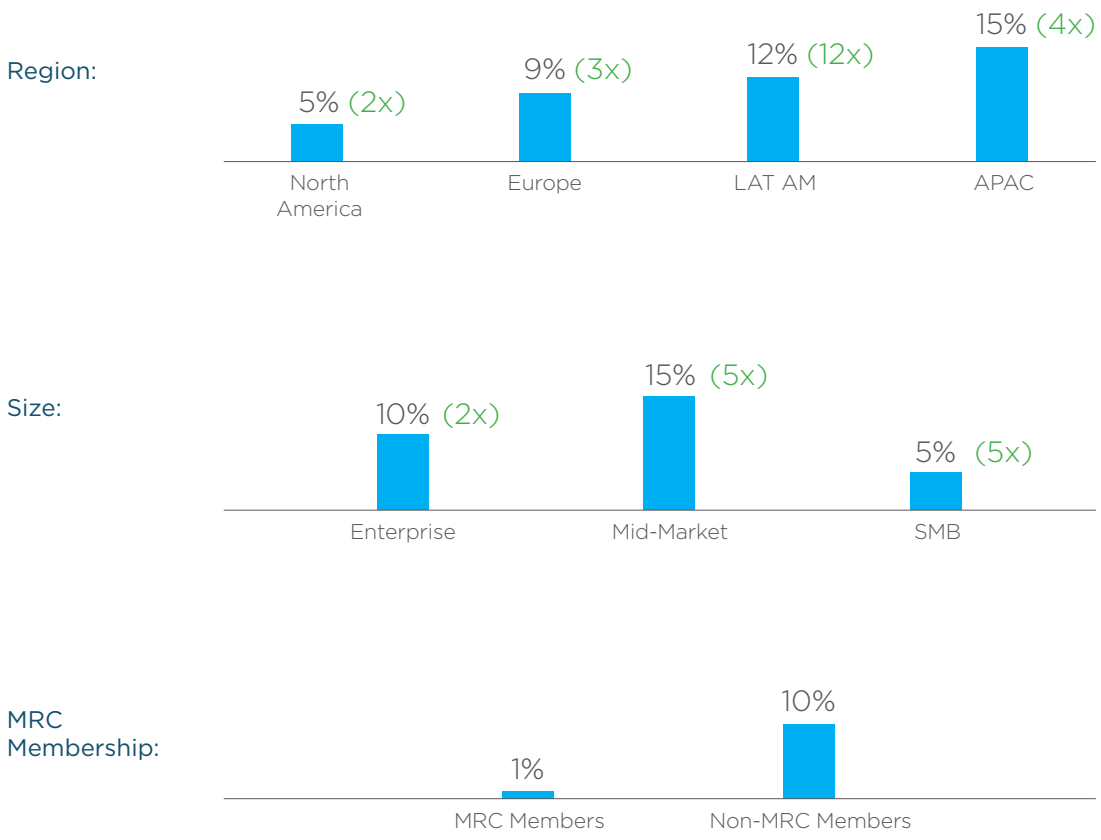


Note: Trimmed medians shown for all cost estimates.

Figure 7

Businesses in Latin America, Asia, and mid-market merchants are seeing fraud management expenses reduce their annual revenues, compared to counterparts in other regions and size segments. MRC members limit fraud management costs far better than non-MRC members, spending relative dimes to dollars but still achieving better results (Figure 8).

% Annual Ecommerce Revenue Spent to Manage Payment Fraud - By Key Breaks



(rate of change increase compared to 2019)

Figure 8

The pattern of increasing fraud attacks, costs, and impacts on merchant organizations becomes clear and unmistakable when one examines the bevy of additional fraud management metrics and KPIs this study has tracked over the past two years. From more revenue being lost to payment fraud to more eCommerce orders being rejected and more eCommerce orders leading to chargebacks, every single indicator for assessing payment fraud impacts has increased since 2019 (see Figure 9).

While these heightened fraud impacts are being felt by merchants worldwide, those in Europe, Asia, and Latin America are the ones being hit hardest, as are mid-market merchants with yearly eCommerce revenues ranging from $5 million to $50 million. Additionally, non-MRC members are clearly feeling the effects of rising fraud to a far greater extent than MRC members. While non-MRC members have always tended to register higher fraud management KPIs, the trend for the other merchant segments highlighted above is more recent. The growing rate of change in fraud management KPIs at the global level is more directly linked to an increase in these metrics among European, Asian, Latin American, and mid-market merchants, than any other merchant segments.

Table Shows Fraud Management KPIs
(Trimmed medians shown for all KPIs)

			By Region - 2021				By Size - 2021			By Membership - 2021	
	2019	2021	North America	Europe	LAT AM	APAC	Enterprise	Mid-Market	SMB	MRC Member	Non-Member
% of eCommerce **revenue lost to payment fraud globally**	2.4	3.1	2.6	3.2	3.7	4.0	3.0	3.4	3.0	0.8	3.4
% of eCommerce **revenue lost to payment fraud from domestic orders**	2.1	3.0	2.5	2.9	3.9	3.9	3.1	3.4	2.7	1.0	3.2
Order rejection rate for domestic orders (%)	2.5	3.0	2.8	2.8	4.0	3.8	3.3	3.7	2.4	2.1	3.2
Order rejection rate for international orders (%)	5.1	5.6	5.0	5.6	6.9	5.7	5.5	6.2	5.1	2.7	5.8
% of eCommerce **orders that turned out to be fraudulent**	2.3	2.6	2.2	2.5	3.5	3.6	2.7	3.0	2.3	0.6	2.8
% of eCommerce **orders that led to chargebacks**	1.3	2.7	2.2	2.6	3.8	3.6	2.9	3.0	2.4	0.7	2.9

Figure 9

The bottom-line takeaways from the insights and trends discussed above: First, eCommerce payment fraud is on the rise, and as a result, merchants are seeing heightened impacts on their online sales and revenues. Second, there is heightened pressure to spend more and to do more to effectively manage and mitigate this growing threat to their business and their customers than they ever have before.

Business Impact of Fraud: In-Depth Insights on Two Key Trends - Manual Review & PSD2

This year's study also uncovered notable findings related to the specific topics of manual order review and the recent rollout of the EU's amendment to the Payment Service Providers Directive, known as PSD2.

Deep Dive into Manual Review:

- While fewer orders are being manually reviewed in 2021, more orders are being declined, especially in APAC.
- Most organizations see a place for manual review in their fraud management strategy, but the vast majority want to reduce their dependency on it.
- While fewer MRC members outsource manual review, their results are similar to non-members (despite a greater share of spend being allocated to review). This may lead to more MRC members eliminating manual review in the future.

Manually reviewing eCommerce orders remains a basic but essential element of virtually any merchant's fraud prevention strategy. The data shows that while the proportion of orders being manually reviewed has decreased from about one-quarter to one-fifth of all eCommerce orders, merchants are now declining a slightly larger share of the orders that they review. Merchants rejected 17% of reviewed orders this year, compared to 12% in 2019 (see Figure 10).

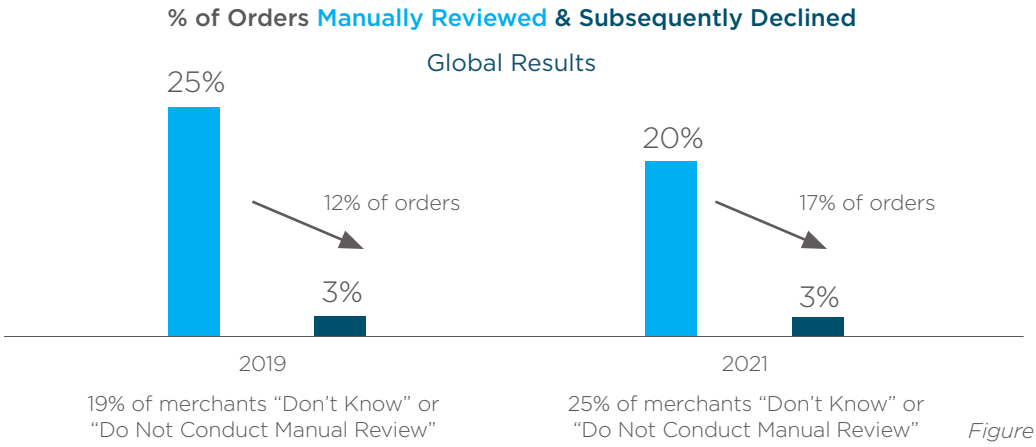
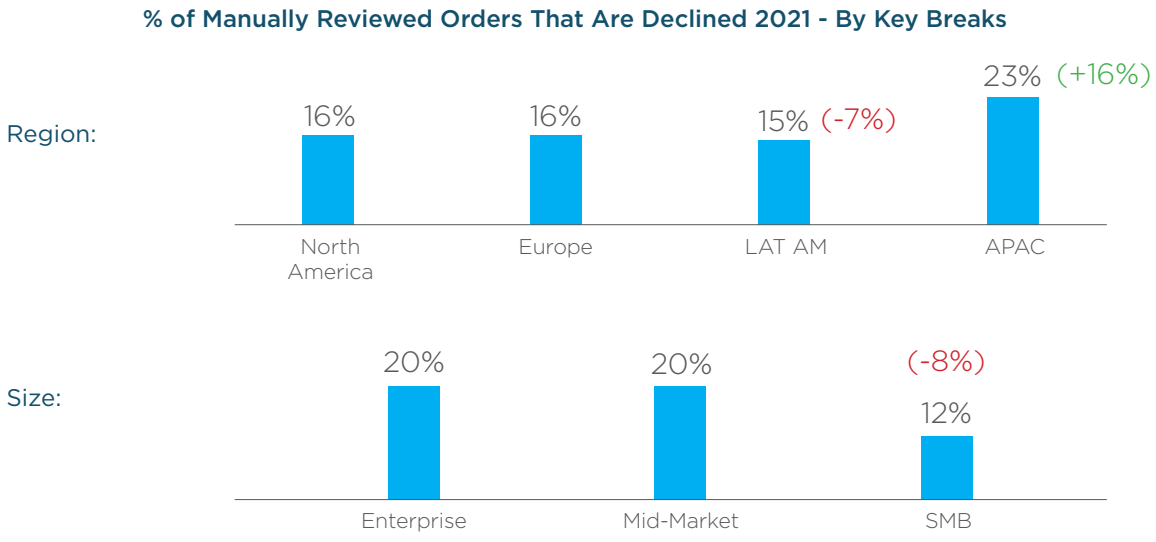


Figure 10

Moreover, while the amount of orders being manually screened is consistent at around 20% for all merchants, globally, the study shows merchants in the APAC region far exceed those in other regions in the share of orders they subsequently reject – a difference that has only taken hold within the past two years, as the share of reviewed orders rejected by merchants in this region rose by 16%. This paints a stark contrast to flat or declining rejection rates by merchants in all other regions, and it may even signal insecurity in systematic and automated rejection decisions by Asia-based merchants, who have been hit harder than most by rising fraud attempts and expenses (as discussed in the previous section).

In addition, the data reveals a recent divergence in the amount of reviewed orders that are declined across merchant size segments: Enterprise and mid-market merchants, being larger and relatively more attractive targets for fraudsters, both reject one-fifth of the orders they review, right on par with their respective rejection rates for 2019. SMB merchants (generating less than $5mn per year), decreased their share of rejected orders by 8% over the past two years and now reject around 12%, on average (see Figure 11). The relative lack of sophisticated fraud measures (including the usage of fewer fraud detection tools) is likely leading to SMB merchants sending a greater proportion of good orders to manual review.



(Parentheses show noteworthy trends compared to 2019: green text indicates an increase & red text indicates a decline)

Figure 11

At a strategic level, manual order review continues to play a pivotal role in merchants' fraud management approaches, as evidenced by the 36% of overall eCommerce fraud management spending merchants earmark for review-related costs, globally (Figure 12). This is relatively consistent with 2019, where 42% of spending was earmarked for review-related costs, globally.

Allocation of Ecommerce Fraud Management Spending

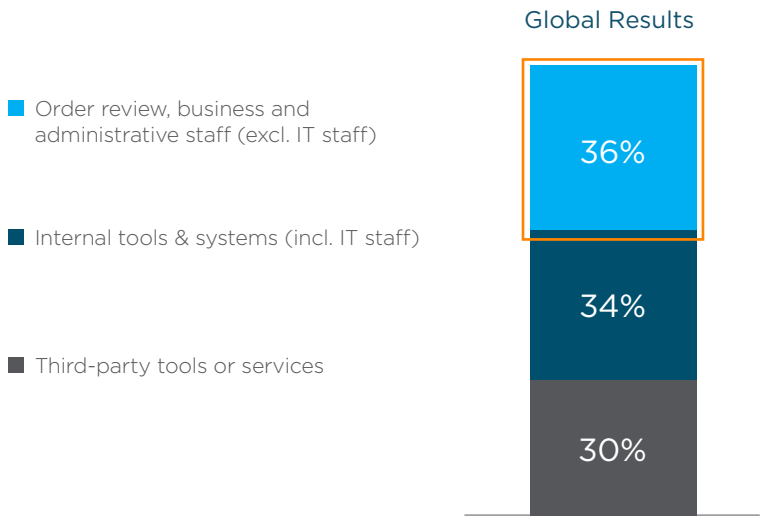
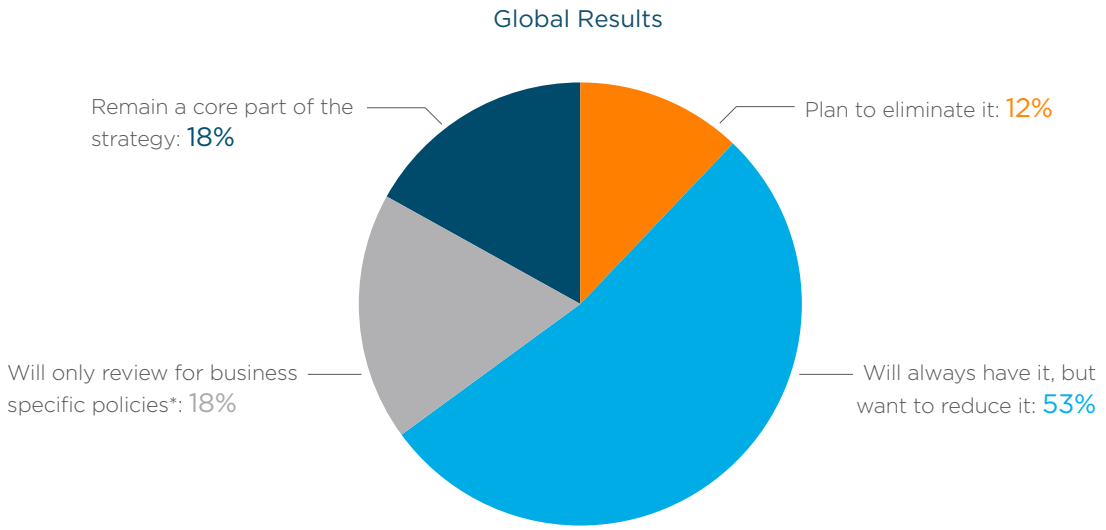


Figure 12

Data gathered from merchants this year indicates that most expect manual review to continue to play a role in their fraud management strategies. The majority, though, plan to reduce the amount of time, labor, and money they devote to this process. Over half (53%) expect that they will always conduct manual review in some form or fashion, but they want to reduce it, while 18% say they will only review for business-specific policies. Another 12% report plans to eliminate manual order review entirely. Less than one-fifth (18%) of merchants plan to retain manual review as a core element of fraud prevention and mitigation for the foreseeable future (Figure 13).

Role of Manual Review In Future Fraud Strategy Plans



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

Figure 13

MRC members also exhibit significant differences in their approaches and attitudes toward manual review, compared to non-MRC members. The former are far less likely to outsource manual review to external parties and also report spending a much greater share of their total fraud management budget on manual review than non-MRC members (51% vs. 36%, as shown in Figure 14).

Despite devoting more resources toward manual review, MRC members review a far smaller share of total eCommerce orders (2% versus 20% for non-members). Members also report identical results to non-members, in terms of the share of reviewed orders they ultimately reject. Increasing awareness among MRC members that they are devoting more resources than non-members to achieve similar (or possibly worse) results may explain why double the proportion of MRC members compared to non-members claim they plan to eliminate manual review from their fraud management strategies (potentially, with a view to outsourcing the manual review function to a third-party).

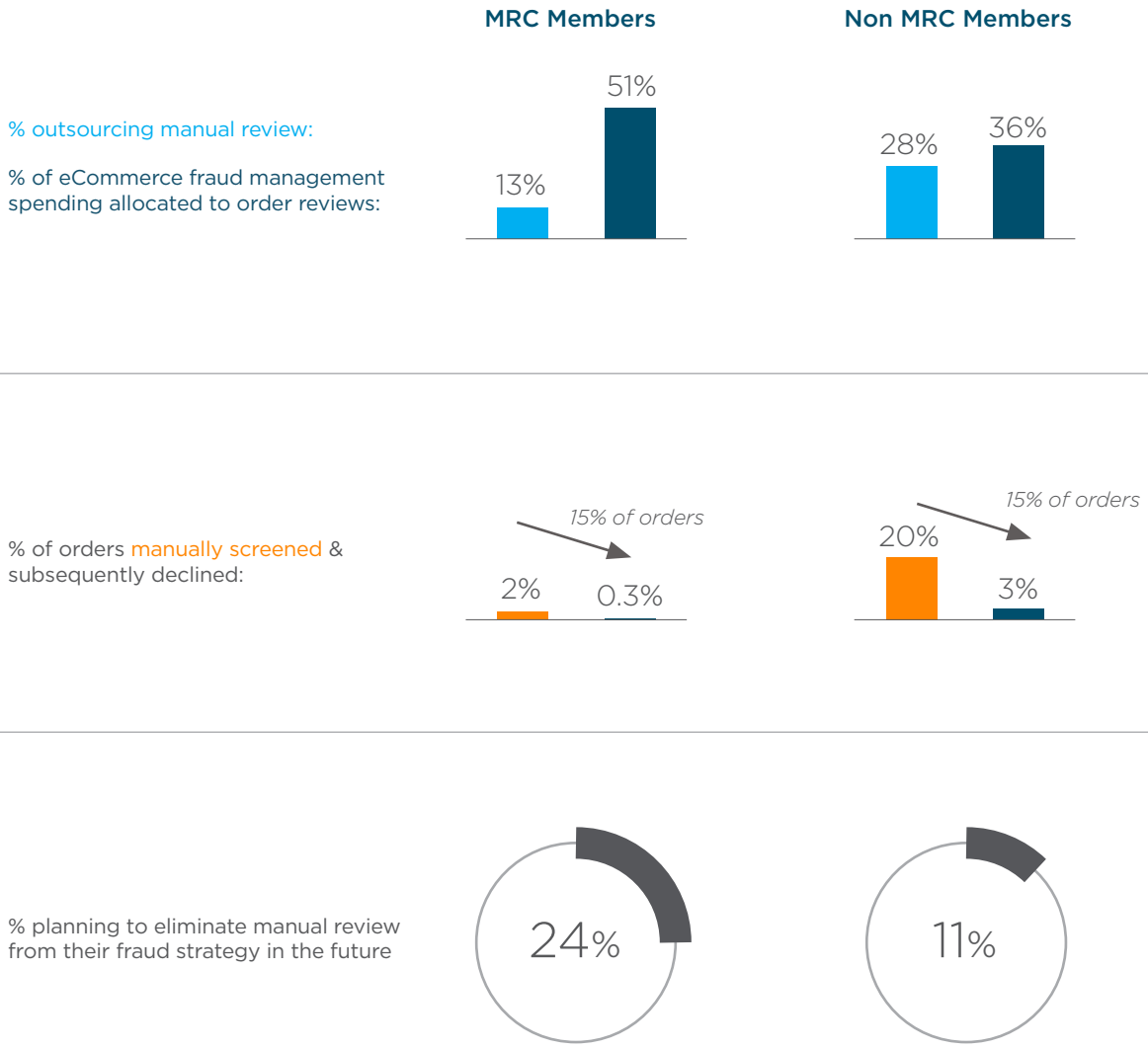


Figure 14

Deep Dive into PSD2:

- Merchants feel increasingly prepared for the amendment to the EU's Payment Service Providers Directive, known as PSD2. Most expect PSD2, in particular strong customer authentication (SCA), to increase the overall complexity of managing both payments and payment fraud.

Turning to the topic of PSD2 and SCA, the data reflects a growing sense of preparedness among merchants, globally. While the proportion of merchants who feel at least somewhat prepared has remained consistent (around 9 in 10 for both 2019 and 2021), now two-thirds claim they feel "very or extremely prepared" for this amendment to PSD2 and the requirements for SCA. This is a significant increase on the 50% who said the same in 2019 (see Figure 15).

Merchant Preparedness For PSD2 - Global Results

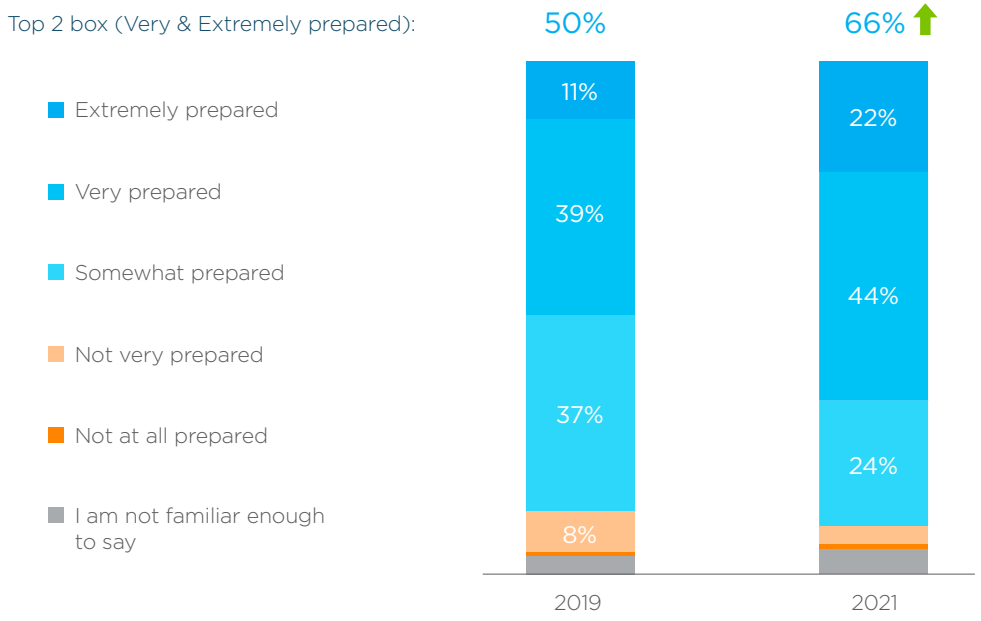


Figure 15

While more merchants now feel at least very prepared for PSD2 and SCA, the share who expect it to have a major impact on their organization remained consistent with 2019, ticking up marginally to 56% this year from 53% two years ago. Specifically, more than half (56%) of merchants expect PSD2 to drive "increased complexity in managing payments," as well as "increased complexity in managing fraud," while just under a quarter (23%) think it will "increase complexity in managing compliance."

However, both merchant preparedness for PSD2 and SCA and expectations that PSD2 and SCA will have a major impact vary across regions and size segments. Merchants based in Europe, Latin America, and APAC are more likely than North American merchants to both feel prepared and to expect PSD2 to have a big impact on their organization. It should be noted, though, that one in ten merchants in our sample from North America are unfamiliar with PSD2 – compared to only 1% of merchants outside of North America - likely because these North American merchants do not operate within the European Union or European Economic Area. Similarly, mid-market and enterprise merchants over-index on both attitudinal metrics, compared to their SMB counterparts (see Figure 16).

MRC members, however, under-index significantly in terms of both feeling prepared and expecting a major impact from PSD2 and SCA, compared to non-MRC members. It should be noted, though, that a much larger portion of MRC members vs. non-members (29% vs. 3%) claim they are not familiar enough to say what kind of impact they expect PSD2 and SCA to have, which is likely driven in part by the high concentration of North American merchants within the MRC member sample for 2021.

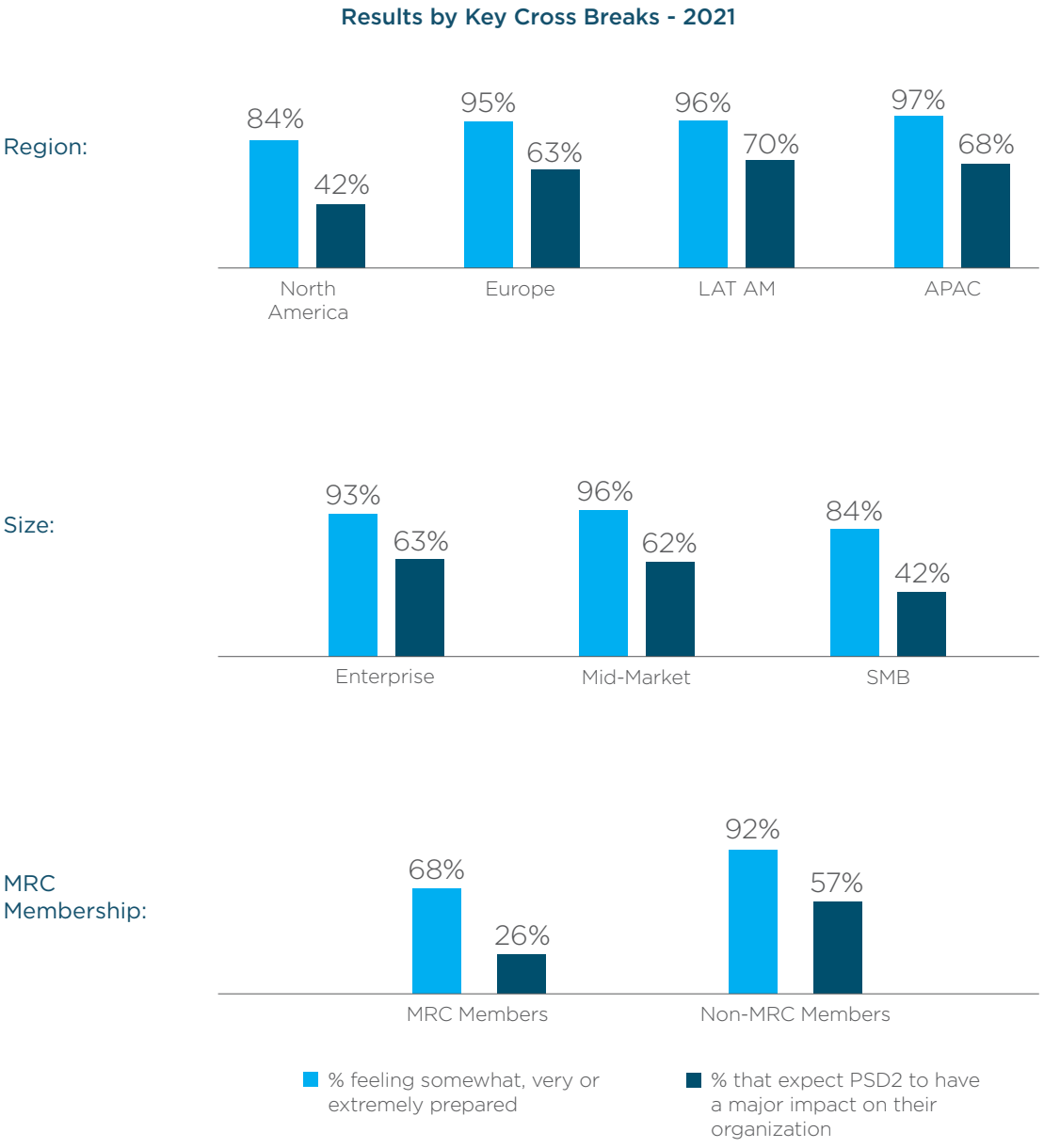


Figure 16

Range of Fraud Attacks: Key Findings

The next area of insights focuses on the volume and variety of fraud attacks experienced by merchants, how those have changed in recent years, and what merchants are doing today to try to minimize their vulnerabilities against the most prevalent and pernicious forms of fraud affecting their organizations, while also grappling with several additional fraud-related challenges.

01 Despite an increase in the volume of fraud attacks, the range of fraud attacks experienced by merchants declined (i.e., they are being attacked more but by fewer types of attacks).

02 Friendly fraud, card testing, phishing, and identity theft are now the most prevalent types of attacks impacting the largest shares of merchants, globally.

- Most merchants have a formal approach in place for combating friendly fraud, with customer notifications and clearly visible policies widely implemented, alongside verifications and reviews of purchase history.
- The prevalence of account takeover attacks has declined per merchant since 2019, in part due to merchants' increased implementation of tools designed to monitor and mitigate this form of fraud.

03 MRC Members have experienced a broader range of fraud attacks, particularly friendly fraud, card testing, account takeover, and triangulation schemes (when compared to non-members).

04 Merchants must grapple with a range of related challenges, beyond detecting and preventing fraud itself and increased costs of fraud management, each of which presents considerable difficulties for merchants to overcome.

As discussed in the first section, three-quarters of merchants saw an increase in the volume of fraud attacks, since the start of the COVID pandemic. Over the same period, however, merchants also saw a decrease in the variety of different fraud attacks experienced by their organization. In 2019, merchants experienced, on average, four different types of fraud attacks, whereas this year, that average dipped to three. In short, merchants are now being hit more often by a more limited range of fraud attacks. One key caveat concerning this trend is that MRC members experience a much broader range of attacks – five, on average – versus non-MRC members, which mirrors the general merchant population with an average of three.

Meanwhile, the most prevalent forms of payment fraud have also shifted significantly since 2019, with friendly fraud – where the customer requested a chargeback from their bank after receiving a purchased product or service – and card testing surpassing phishing / pharming and identity theft as the top two most common attacks impacting merchants. Friendly fraud has become particularly problematic for merchants in North America and APAC, where reported incidence rates rose by 9% and 16%, respectively, compared to 2019. Figure 17 contains detailed data on the most common types of fraud attacks and the differences in incidence rates for MRC members versus the global merchant population.

	2019 Rank	2021 Rank	Global % Experiencing (2021)	% of MRC Members Experiencing (2021)
Friendly Fraud	5	1	39%	92%
Card Testing	4	2	37%	84%
Phishing / Pharming / Whaling	1	3	34%	34%
Identity Theft	2	4	28%	37%
Coupon / Discount / Refund Abuse	7	5	27%	39%
Loyalty Fraud	10	6	27%	24%
Account Takeover	3	7	23%	66%
Affiliate Fraud	6	8	21%	16%
Triangulation Schemes	11	9	20%	55%
Botnets	8	10	19%	37%
Money Laundering	12	11	16%	18%
Re-Shipping	9	12	15%	26%

= Declining Rank = Increasing Rank = Sig. Higher

Figure 17

There does exist some variation in the most common fraud attacks impacting merchants in different regions and size segments, as indicated by the respective rankings shown in Figure 18. But, while it is important to take note of these segment-specific differences and nuances, this data also underscores the universal prevalence and relevance of friendly fraud, phishing / pharming, and card testing as the three types of payment fraud that virtually all merchants are most likely to experience, regardless of geographic area or online revenue.

Top Fraud Attacks Experienced by Region

	North America	Europe	LAT AM	APAC
1	Card testing	Phishing/ pharming/whaling	Friendly fraud	Phishing/ pharming/whaling
2	Friendly fraud	Friendly fraud	Card testing	Friendly fraud
3	Phishing/ pharming/whaling	Account takeover	Coupon/discount/ refund abuse	Loyalty fraud
4	Identity theft	Loyalty fraud	Phishing/ pharming/whaling	Identity theft
5	Coupon/discount/ refund abuse	Card testing	Affiliate fraud	Card testing Coupon/discount/ refund abuse

Top Fraud Attacks Experience by Company Size

	SMB	Mid-Market	Enterprise
1	Friendly fraud	Friendly fraud	Friendly fraud
2	Card testing	Card testing	Card testing
3	Phishing/ pharming/whaling	Identity theft	Phishing/ pharming/whaling
4	Identity theft	Phishing/ pharming/whaling	Loyalty fraud
5	Coupon/discount/ refund abuse	Coupon/discount/ refund abuse	Coupon/discount/ refund abuse

Figure 18

Globally, friendly fraud is now the #1 most common type of attack experienced by merchants, who estimate that around 1.2% of their accepted eCommerce orders eventually turn out to be friendly fraud. Friendly fraud is a greater concern for merchants in Latin America and Asia (given the % of accepted orders that turned out to be friendly fraud), while fewer accepted orders for MRC members turn out to be friendly fraud (Figure 19).

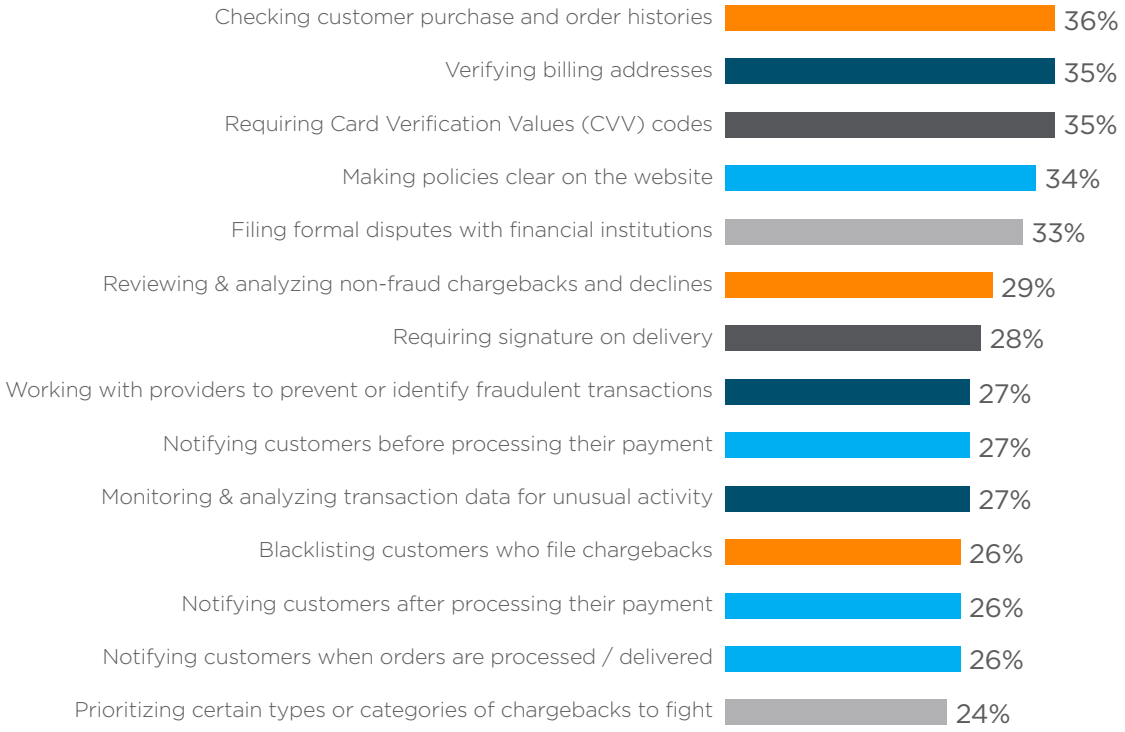
	Region - 2021				Size - 2021			Membership- 2021	
	North America	Europe	LAT AM	APAC	Enterprise	Mid-Market	SMB	MRC Members	Non-MRC Members
% of Accepted Orders That Turned Out to be Friendly Fraud	1.0	1.3	1.6	1.5	1.3	1.4	1.0	0.4	1.2

Figure 19

How are merchants responding to the rise in friendly fraud attacks on their organizations over the past two years?

80% of merchants globally have a formal approach for combating friendly fraud (although this is true for only 71% of merchants in North America and 68% of SMB merchants). Among the 4 in 5 merchants who have formal strategies in place, most have opted for a multi-pronged approach, comprising a range of specific tactics, such as customer notifications, clear payment and return policies, and various verification measures designed to check and confirm customer identities (Figure 20).

Current Approaches Used to Combat Friendly Fraud - 2021



Grouped Approaches: % selecting at least one

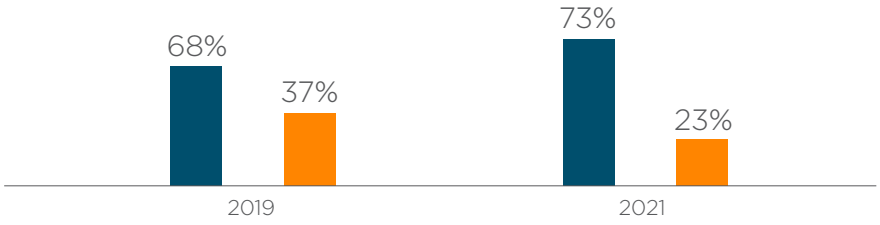
Notifications & Visibility	68%
Verification & Identification	61%
Flagging & Checking	60%
Enhanced Requirements	52%
Filing & Fighting	47%

Figure 20

While friendly fraud is on the rise for merchants, account takeover fraud – i.e., when fraudsters illegally access or manipulate customer account data – is on the decline. In 2019, account takeover was the third most common fraud attack, experienced by 37% of merchants. But this year, account takeover fell to #7 overall, and impacted less than a quarter (23%) of merchants globally (Figure 21).

Part of the decrease in account takeover fraud may be attributed to the adoption of specialized tools to monitor and prevent this form of attack, as the share of organizations with these tools in place rose significantly. North American merchants and SMBs appear to be lagging behind merchants in other regions and size segments when implementing these specialized tools (see figure 21).

Global % of Organizations With Tools to Monitor Account Takeover Fraud &
% of Organizations Experiencing Account Takeover Fraud



% With Tools in Place in 2021 - By Key Cross Breaks

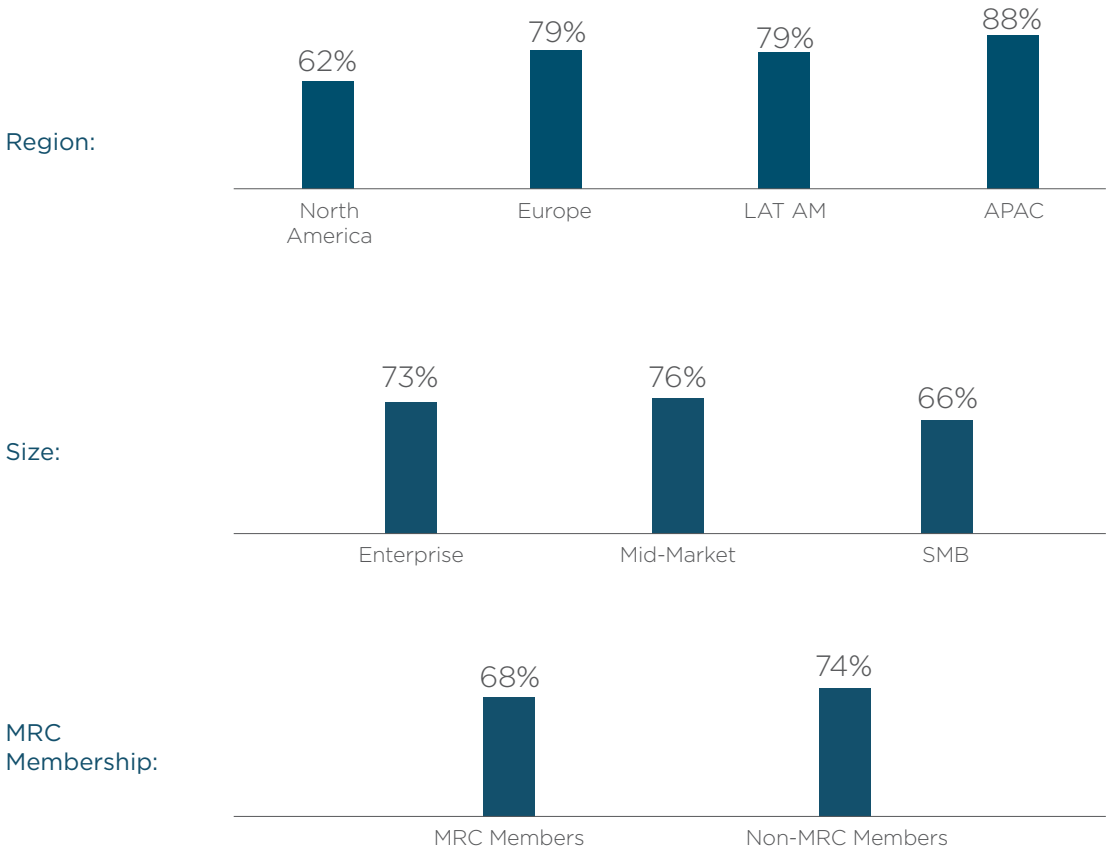


Figure 21

One factor that makes eCommerce fraud management highly difficult and complex for merchants is that they must grapple with a range of business challenges, beyond just monitoring and preventing payment fraud itself. Figure 22 illustrates the range, the relative incidence, and the severity of these fraud management challenges. These challenges impact 92% of merchants, globally.

Incidence & Severity of Fraud Management Challenges Experienced by Merchants in The Past 12 Months

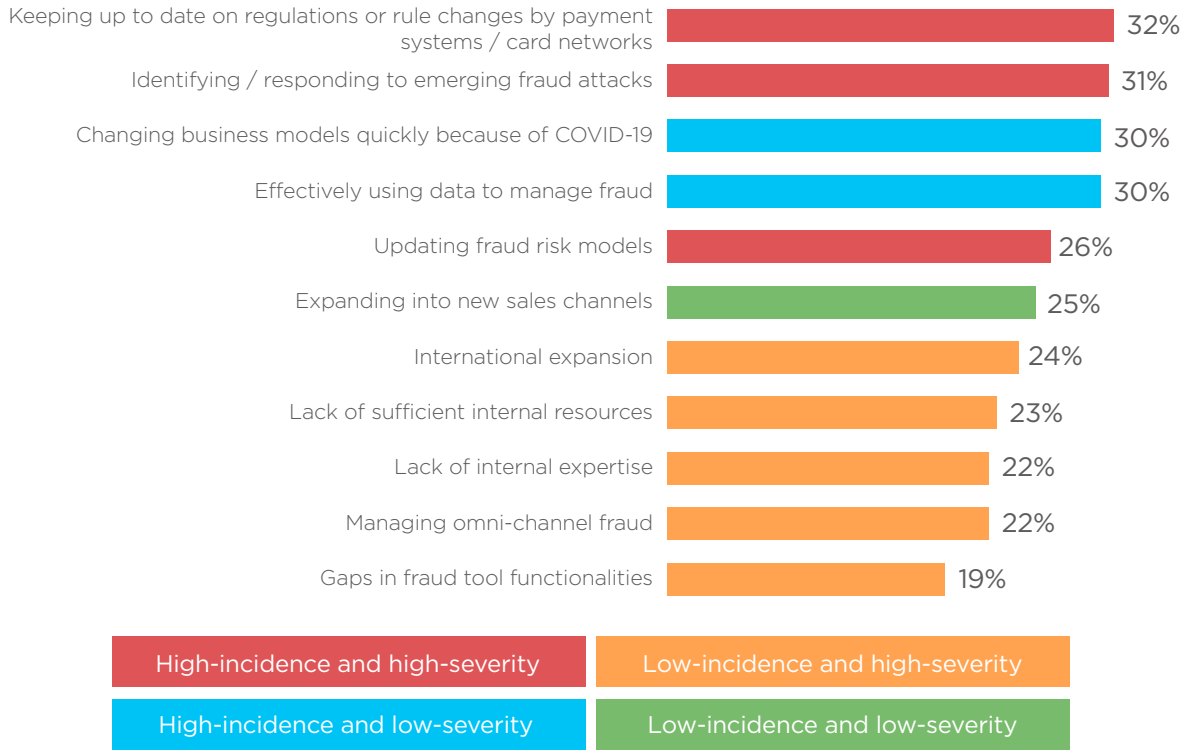


Figure 22

The average merchant in 2021 has experienced at least three challenges shown above in the past 12 months, and many are struggling to overcome several at once. Enterprises, for instance, are far more likely to face the majority of the challenges listed in Figure 22, compared to mid-market and SMB merchants: Over a quarter (26%) of enterprise merchants observed five or more of the challenges above in the past year, versus 12% of mid-market and 9% of SMB merchants.

MRC members also face more fraud-related challenges than non-members, as 39% of the former experienced five or more challenges in the past year, compared to 15% of the latter. MRC members are far more apt than non-MRC members to cite frustrations with lack of internal resources (50% vs. 21%) and gaps in fraud tool functionalities (45% vs. 17%).

Each fraud management challenge presents varying degrees of severity and/or difficulty to merchant organizations. While three of the top five most prevalent challenges are also considered the most severe, there is a second set of highly pernicious problems, indicated by the orange bars in Figure 22, each of which impacts a smaller share of merchants, globally. It is important to acknowledge that these issues may be as problematic for those merchants that experience them as the more widely felt challenges atop the list.

The results suggest effectively combating eCommerce fraud means reducing the volume of attacks targeting merchant organizations, understanding and combating multiple different types of fraud attacks as they continue to evolve and emerge, and overcoming a bevy of additional fraud-related challenges that hamper and constrain each merchant's fraud prevention capabilities to varying extents.

Fraud Prevention Strategies: Key Findings

The final area of this report looks at merchants' fraud prevention strategies. How are merchants addressing and combating eCommerce payment fraud, now and in the future?

01 Despite the increase in attacks and revenue lost, merchants are prioritizing improvements to the customer/shopping experience as part of their fraud management practices (as opposed to minimizing fraud-related operational costs, for example).

02 At a tactical level, merchants are rationalizing their fraud management toolkits, relying more heavily on just a handful of widely used tools, compared to 2019.

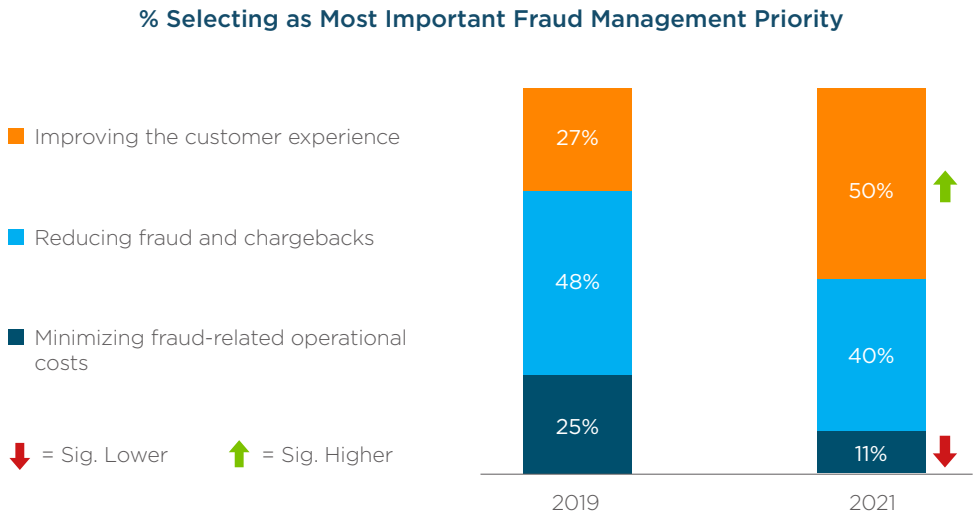
03 MRC Members are using a broader range of fraud detection tools than non-members, which may partly explain why they experience (i.e., detect) a greater range of fraud attacks (as demonstrated in the "range of fraud attacks" section of this report).

04 Except for CVN, two-factor phone authentication, and 3DS authentication, many of the most effective fraud detection tools (in the view of participants in the survey) are not the most widely used, nor are they the most likely to be adopted in the future.

Fundamental to understanding merchants' fraud prevention strategies is knowing what goals or objectives they prioritize, relative to others, in their fraud management approaches. In 2019, the data showed merchants were most likely to see reducing fraud and chargebacks as the primary strategic goal when it came to fraud management.

This year half of merchants are now choosing to prioritize improving their customer experience (CX), compared to 40% who continue to prioritize their focus on fraud reduction and a mere 11% that are mainly concerned with minimizing costs (see Figure 23). Notably, this strategic shift is even starker for MRC members versus non-members, as 68% of the former are focused on improving CX, versus 48% of the latter. Non-MRC members continue to be more concerned with reducing fraud and chargebacks, as evidenced by the 40% who selected this as their primary fraud prevention objective (versus just 29% of MRC members).

Figure 23 also illustrates a few noteworthy differences in which strategic goals merchants are choosing to de-prioritize, across different regions, size tiers, and industry sectors. As merchants focused more on CX improvement in their fraud management decisions, merchants in Latin America and at the enterprise level have tended to put less emphasis on fraud and chargeback reduction. European, mid-market, and SMB merchants, and those focused on selling digital goods and travel & tourism-related products and services, have been more apt to focus less on minimizing fraud-related operational costs. Merchants in North America and APAC, as well as those selling physical goods in retail sectors, are equally likely to de-emphasize both fraud and cost reduction, as they prioritize improving their customer experience.



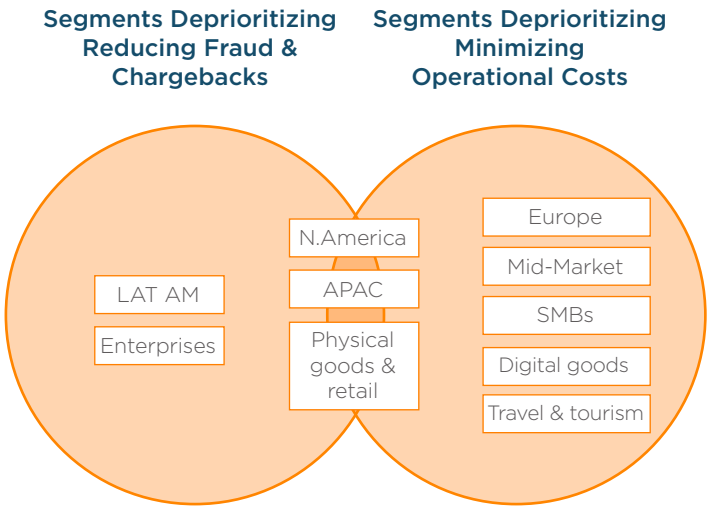


Figure 23

This strategic shift in merchants' fraud management aims to strike a better balance between protecting the assets and operations of the business and delivering a high-quality shopping and payment experience for customers.

Over the past two years, merchants' fraud prevention strategies have evolved at the organizational level, and correspondingly, so has the quality of their fraud management toolkits at the tactical level. Instead of continuing to implement an array of new anti-fraud tools and technologies, merchants have opted to rationalize fraud prevention solutions. The average number of tools each merchant has in place has dropped by half, from 10 in 2019 to 5 this year.

It is important to highlight that MRC members represent a notable exception to this trend, as they still report having 11 tools in place, on average. Figure 24 illustrates the stark difference in the size and breadth of fraud prevention toolkits between MRC members and the global merchant population, with MRC members continuing to utilize a much wider array of tactical solutions than the average merchant. Figure 24 also shows how most widely used fraud detection tools have remained quite consistent over the past two years, with CVN, email and address verification, as well as customer order histories and 3-D Secure Authentication comprising the top five tools used by the largest shares of merchants in both years, worldwide.

Top 15 Fraud Detection Tools Used	2019 Rank*	2021 Rank*	Global % Using Tool (2021)	% of MRC Members Using Tool (2021)
CVN (Card Verification Number)	2	1	54%	76%
Email verification	3	2	43%	58%
Customer order history	1	3	38%	79%
Address Verification Service (AVS)	4	4	37%	79%
3-D Secure authentication	5	5	36%	55%
Telephone number verification / reverse lookup	13	6	31%	50%
Postal address validation services	8	7	27%	53%
Negative lists / blacklists (in-house lists)	6	8	24%	84%
Customer website behavior / pattern analysis	10	9	23%	42%
Positive lists / whitelists	9	10	21%	71%
Order velocity monitoring	19	11	21%	76%
Geographic indicators / maps	17	12	18%	58%
Geo location for country / city, etc.	7	13	18%	74%
Two-factor phone authentication (In-App, SMS, etc.)	11	14	18%	29%
Social networking sites	18	15	18%	39%

**North America & Europe only (for consistent tracking)*

= Declining Rank = Increasing Rank = Sig. Higher

Figure 24

The most prevalent fraud detection tools are also fairly consistent across regions and size segments, as illustrated in Figure 25. But there are a few notable differences in the types and numbers of tools most relied on by merchants in each group: For instance, those in Europe and APAC are more likely than those in North America to have implemented 3DS Authentication (greater adoption in Europe is likely driven by merchants needing to comply with SCA and PSD2 and in APAC given the higher volume of fraud attacks experienced, as noted earlier in this report). Also, enterprise merchants understandably rely on a larger array of fraud detection tools than mid-market & SMB merchants, on average.

Top Fraud Detection Tools Used by Region

Top Fraud Detection Tools Used by Company Size

	North America	Europe	LAT AM	APAC	SMB	Mid-Market	Enterprise
1	CVN	CVN	Email verification	3DS auth./ SafeKey	CVN	CVN	CVN
2	Email verification	3DS auth./ SafeKey	CVN	CVN	Email verification	3DS auth./ SafeKey	Email verification
3	Customer order history	Email verification	Customer order history	Email verification	Customer order history	Email verification	AVS
4	AVS	AVS	AVS	Phone number verification	AVS	Customer order history	3DS auth./ SafeKey
5	Phone number verification	Customer order history	Credit history check	AVS	Postal address validation	AVS Phone number verification	Customer order history
Avg. # of detection tools used	5	4	6	6	4	4	6

Figure 25

As merchants continue to evaluate and implement new anti-fraud tools in the future, it will behoove many to keep in mind the final two figures in this section, below, which segment 25 fraud prevention tools, based on how widely used they are and, importantly, how effective merchants say they are at detecting and preventing fraud. Figure 26 shows current usage and planned adoption rates for tools that merchants consider most effective at thwarting fraud, while Figure 27 shows the same statistics for tools that merchants say are less effective, on average.

% Currently Using & Planning to Adopt "More Effective" Fraud Detection Tools

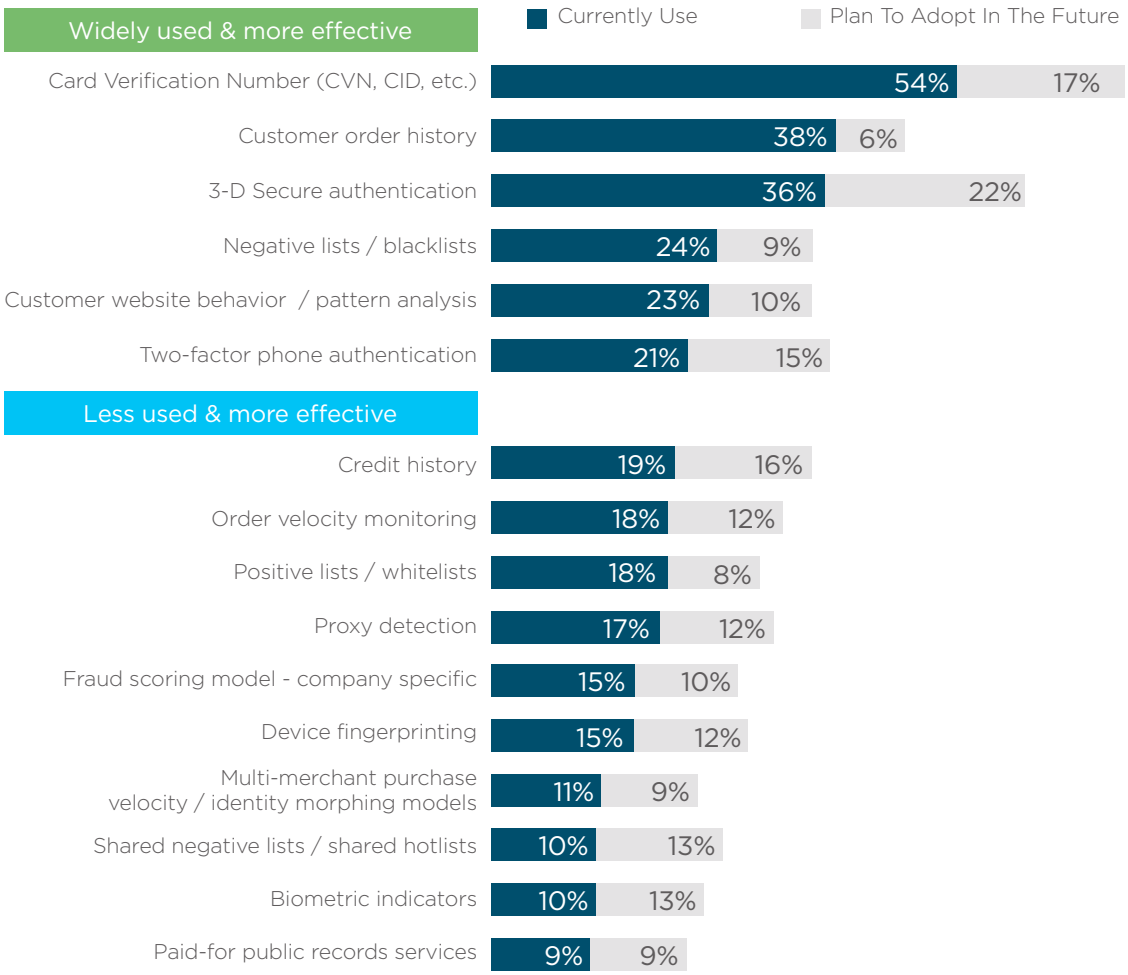


Figure 26

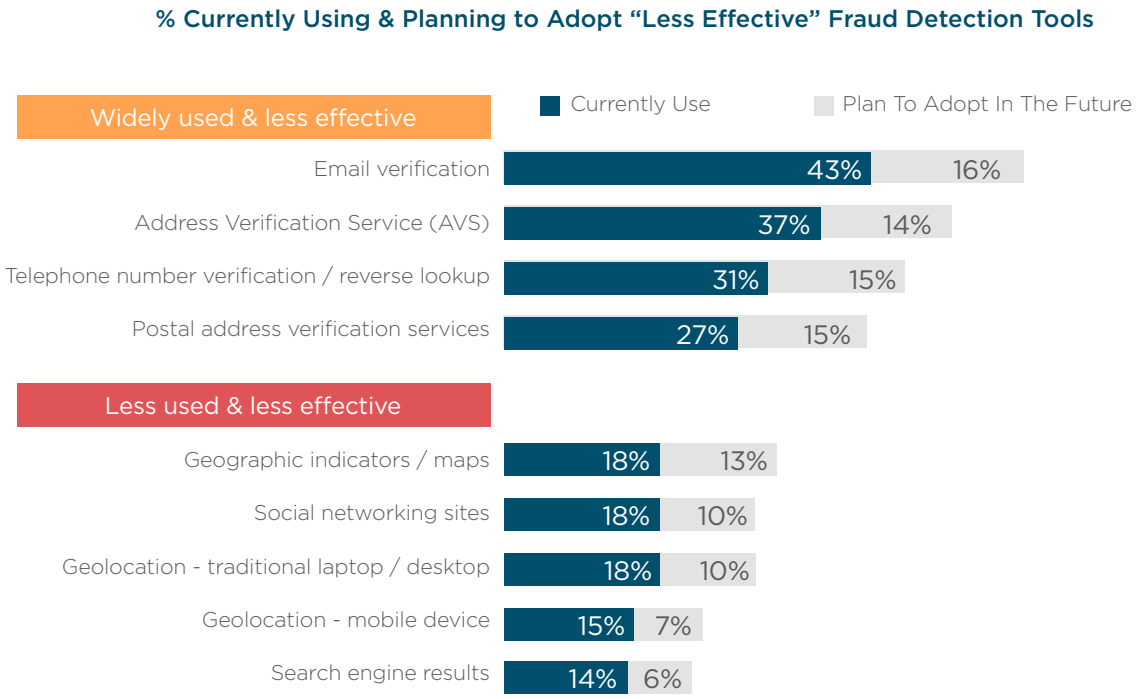


Figure 27

Figures 26 and 27 should sound a cautionary note to merchants about their future investment decisions in anti-fraud solutions at the tactical level: The data above show that many of the most effective fraud detection tools are not the most widely used, today, nor are they the most likely to be adopted by merchants, in the future. To advance their anti-fraud capabilities and achieve the best results at the tactical level, merchants should consider investing in tools that may not be as widely used as many others, yet are generally seen as more effective, such as credit history checks, order velocity monitoring, positive / whitelists, proxy detection, device fingerprinting and company-specific fraud-scoring models.

Conclusion

The key results and findings discussed in this report highlight how critical, complex, and challenging the issue of global eCommerce payment fraud has become for merchants. The report illustrates several positive trends and indicators that together send a positive and encouraging signal about merchants' collective capabilities to successfully improve and advance both fraud management strategies and tactics to better protect their organizations, as well as their customers, from fraud-related threats and harms, in the future. The MRC is committed to supporting merchants' fraud management and prevention efforts by continuing to sponsor and publicize further research and analysis on these important topics, in the years to come.

About The Authors

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

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

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 – 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. By 'eCommerce', we mean any channel through which a customer can place a non-store order. This may be through your website or a mobile device.*

Figure 3 – *"channel supported": Which of the following order channels does your organization support?*

Figure 3 – *"fraud tracked": For which of the following channels does your organization track payment fraud?*

Figure 4: *How important is eCommerce fraud management to your organization's overall business strategy?*

Figure 5 & 6:

- COVID impact on fraud attempts: *To what extent do you believe the COVID pandemic has impacted the volume of fraud attempts made on your organization?*
- COVID impact on fraud rate by revenue: *How has the COVID pandemic impacted your annual eCommerce revenue lost due to payment fraud globally, i.e., fraud rate by revenue?*

Figure 7 & 8: *Please indicate the percent of your annual eCommerce revenue your organization spends to manage payment fraud — excluding actual fraud losses.*

Figure 9:

- % of eCommerce revenue lost to payment fraud globally: *Please indicate the percent of your annual eCommerce revenue lost due to payment fraud globally, i.e., fraud rate by revenue.*
- % of eCommerce revenue lost to payment fraud from domestic orders: *Please indicate the percent of your annual eCommerce revenue lost due to payment fraud on domestic orders.*
- Order rejection rate for domestic orders: *Please indicate your order rejection rate for domestic orders i.e., the percentage of these orders rejected due to suspicion of fraud.*
- Order rejection rate for international orders: *Please indicate your order rejection rate for international orders the percentage of these orders rejected due to suspicion of fraud.*
- % of eCommerce orders that turned out to be fraudulent: *Please indicate the percent of accepted annual eCommerce orders that turned out to be fraudulent.*
- % of eCommerce orders that led to chargebacks: *Please provide the percent of eCommerce orders for which you have received chargebacks due to fraud in the past 12 months.*

Figure 10:

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

Figure 11: % of manually reviewed orders that are declined: *Of the eCommerce orders manually reviewed by your organization, please indicate the percentage you decline (cancel) due to suspicion of fraud*

Figure 12: Allocation of eCommerce fraud management spending: *Please indicate the percent of your current annual eCommerce fraud management spending that is allocated to each of the following areas.*

Figure 13: Role of manual review in future fraud strategy plans: *How do your organization's future fraud strategy plans incorporate manual review?*

Figure 14:

- % outsourcing manual review: *Which of the following fraud management functions, if any, does your organization outsource? [response option: Manual review].*
- % of eCommerce fraud management spending allocated to order review: *Please indicate the percent of your current annual eCommerce fraud management spending that is allocated to Order review, business and administrative staff (excluding IT staff)*
- % of orders manually reviewed: *Please indicate the percentage of eCommerce orders you manually screen for fraud.*
- % of orders subsequently declined: *Of the eCommerce orders manually reviewed by your organization, please indicate the percentage you decline (cancel) due to suspicion of fraud.*
- % planning to eliminate manual review from their fraud strategy in the future: *How do your organization's future fraud strategy plans incorporate manual review? [response option: They don't, we plan to eliminate manual review].*

Figure 15: How prepared would you say your organization is for PSD2?

Figure 16:

- Preparedness for PSD2: *How prepared would you say your organization is for PSD2?*
- % that expected PSD2 to have a major impact on their organzation: *What type of impact do you expect PSD2 to have on your organization? [Response option: Major impact]*

Figure 17 & 18: *Which of the following types of fraud attacks, if any, have you ever experienced at your organization?*

Figure 19: *Please indicate the percent of accepted annual eCommerce orders over the past 12 months that turned out to be friendly fraud / chargeback fraud i.e. where the customer requested a chargeback from their bank after receiving the purchased product/service.*

Figure 20: *Which of these describe your organization's current approach to combating friendly fraud / chargeback fraud, i.e. when a customer requests a chargeback from their bank after receiving the purchased product/service?*

Figure 21:

- % of organizations with tools in place to monitor account takeover fraud: *Do you have tools in place to monitor account takeover fraud during the customer account creation and login process? [Response option: Yes]*
- % of organizations experiencing account takeover fraud: *Which of the following types of fraud attacks, if any, have you ever experienced at your organization?*

Figure 22:

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

- Severity of fraud management challenges: *And how challenging would you say each of the following have been for your organization to manage? [Scale ranged from extremely challenging to not at all challenging]*

Figure 23: *Which one fraud management practice would you say is the most important to your organization when evaluating fraud management practices*

Figure 24 & 25: *Please indicate which fraud detection tools your organization currently uses.*

Figure 26 & 27:

- Tools currently used: *Please indicate which fraud detection tools your organization currently uses.*

- Tools organizations plan to adopt in the future: *You indicated that your organization does not currently use any of the following fraud detection tools. Which tools, if any, does your organization have plans to start using in the future?*

- Effectiveness of tools: *Now, how effective is each of the following tools in detecting eCommerce payment fraud? [Scale ranged from extremely effective to not at all effective]*

For more information about MRC, please visit:
merchantriskcouncil.org

MRC
Building
Better Commerce
Fraud & Payments Professionals