



GLOBAL FRAUD SURVEY RESULTS •2019•



In partnership with

CyberSource®
A Visa Solution



Building
Better Commerce
Fraud & Payments Professionals

ABOUT

ABOUT CyberSource

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 fulfill their brand promise. For more information, please visit cybersource.com.

ABOUT MRC

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.

ABOUT GfK

GfK is the trusted source of relevant market and consumer information that enables its clients to make smarter decisions. More than 13,000 market research experts combine their passion with GfK's long-standing data science experience. This allows GfK to deliver vital global insights matched with local market intelligence from more than 100 countries. GfK turns big data into smart data, enabling its clients to improve their competitive edge and enrich consumers' experiences and choices. As a research and analytics partner, GfK promises its clients all over the world "Growth from Knowledge."

INTRODUCTION

The Merchant Risk Council (MRC) is pleased to present the results of the 2019 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.

This year's survey was undertaken with the goal of providing a substantially broader perspective on the current state of fraud management and the eCommerce fraud landscape. Representing a wider array of global eCommerce merchants than ever before, the survey captured the views of more than 2,800 fraud management specialists from small, mid-market and enterprise-level organizations in five verticals. Responses were intentionally drawn from a wider sampling of eCommerce merchants—based on global quotas set by size of company according to annual sales—to capture a more holistic picture of fraud today.

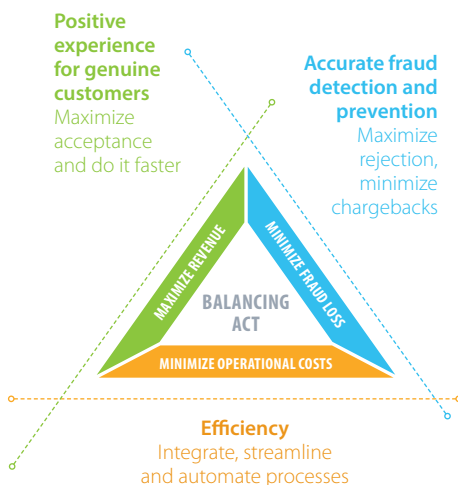
FINE-TUNING THE THREE PILLARS OF FRAUD MANAGEMENT

Developing and maintaining effective eCommerce fraud management systems requires a careful balancing act. Staying ahead of the curve in a dynamically changing online marketplace—by accounting for shifting fraud patterns and making sure their fraud operations are streamlined and efficient—allows merchants to ensure that their shopping experience meets customer expectations.

There are three pillars of effective fraud management:

- **Maximizing revenue**
- **Minimizing fraud loss**
- **Minimizing operational costs**

Finding the right point of balance between these three key pillars of fraud management is critical, but maintaining that balance is a hands-on job of careful calibration—as each business' balance point is unique.



Less than
20%
of all businesses
give equal weight
to all three pillars

SHARING TOP PERFORMERS' BEST PRACTICES

The survey revealed that merchants who see all three pillars of fraud management as equally important fare better against fraud than those who don't. Less than 20% of all businesses give equal weight to all three pillars, but those who do set themselves apart statistically—outperforming other merchants on key metrics. These merchants are the Top Performers in eCommerce fraud management.

This report identifies the key attributes, behaviors and fraud management philosophies of these Top Performers and offers insights, tips and best practices that the MRC merchant community can apply to their own fraud management strategies going forward.

EXECUTIVE SUMMARY

Top Performers have a unique perspective on fraud management that delivers serious results. Here's what it takes to become a fraud management leader.

Only **18%**
rated all three pillars as
extremely important
—these are the
Top Performers

ALL RESPONDENTS WERE ASKED:

How important is each of the following to your organization when designing your fraud management strategies?

- Improving the customer experience
- Reducing fraud and chargebacks
- Minimizing fraud-related operational costs

TOP PERFORMERS—THOSE WHO RATE ALL THREE PILLARS AS *EXTREMELY IMPORTANT*—REPORT THEY DO BETTER, ON A STATISTICALLY SIGNIFICANT BASIS, ACROSS THE FOLLOWING ASPECTS OF FRAUD MANAGEMENT:



Are **more than twice (2.37 times)** as likely to rate **eCommerce fraud management** as extremely important to their organization's overall business strategy.
(83% vs. 35% for others)



Have a **greater range of capabilities**, giving them agility to respond to the dynamic landscape in which they operate.



Less likely to be challenged by emerging attacks, the #1 challenge for all, as well as updating risk models, gaps in fraud tool functionalities and managing omnichannel fraud.



More likely to recognize the need for improvement in how their organization uses data to manage fraud.
(64% vs. 55% for others)



Fewer engage in manual review; of those that do, they spend less time (per order) and money (share of budget) on it.



Have a fraud coded chargeback rate **4 times lower**.
(0.1% vs. 0.4% for others)

1. Results are self-reported by survey respondents



MRC members had a
higher-than-average
concentration of
Top Performers at
20%

The survey revealed six key ideas that can help MRC members better understand the eCommerce fraud landscape and how to develop more effective fraud management strategies moving forward.

- 1 eCommerce fraud management is integral to business strategy, yet only around 4 in 10 say it is extremely important to their business
- 2 Organizations who prioritize fraud management balance fare significantly better
- 3 Responding to emerging attacks ranks as the #1 challenge over the past year—and considerable room for improvement exists in using data to manage fraud
- 4 Manual review remains essential, though it takes a toll on businesses, eating up roughly 40% of eCommerce fraud management budgets
- 5 Top fraud attacks will continue to evolve
- 6 Widespread dissatisfaction is driving desire to invest in additional tools

This report examines what merchants can learn from these six key developments concerning the future of fraud management, evaluating how MRC members think about and practice fraud management. It also looks at Top Performers' behaviors and attitudes to discover what tactics and best practices MRC members can implement in their fraud management strategies as they fine-tune their own balance points.



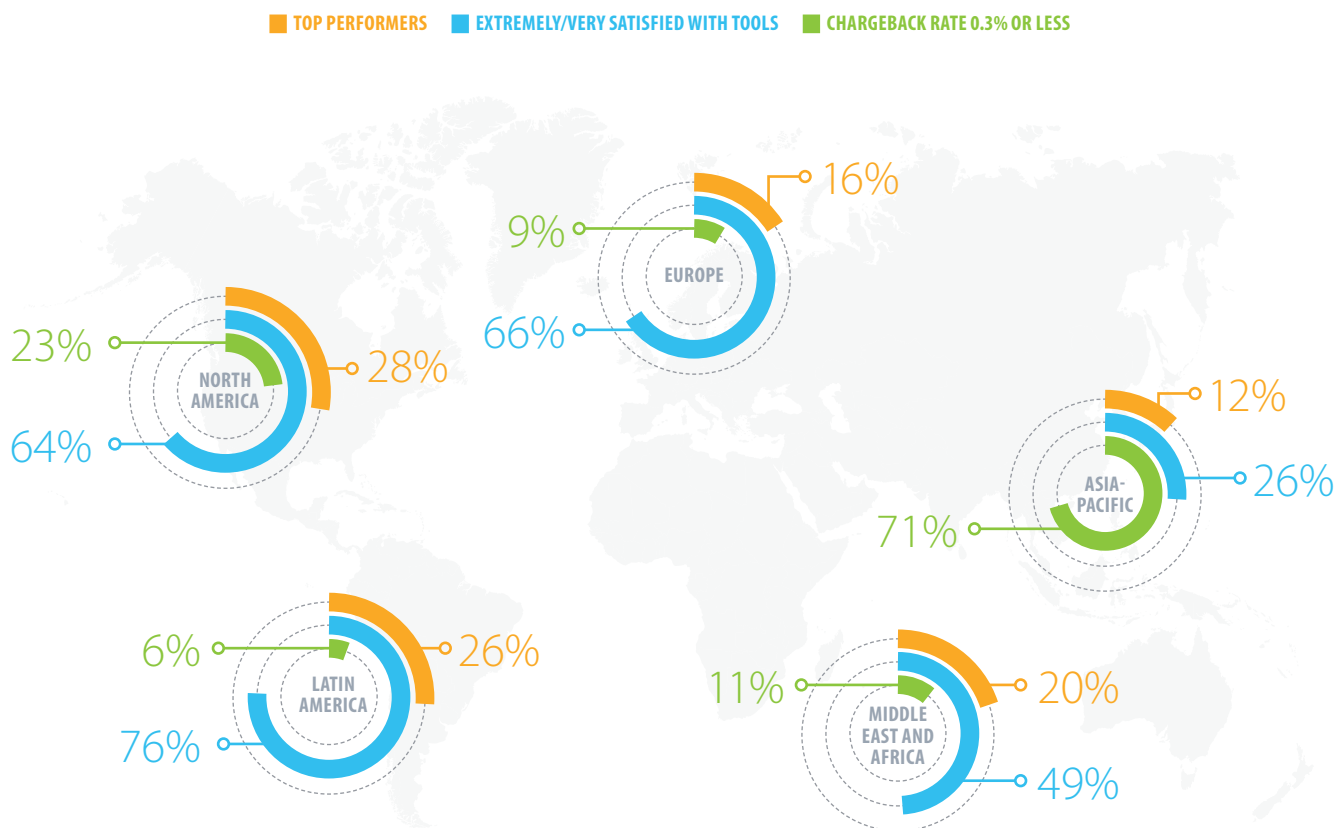
Top Performers put
a greater focus
on analytics and
automation

CALIBRATION IN CONTEXT

The final section of the report discusses the top tools that MRC members are using today as well as the ones they plan to add in the future, followed by a look at how the Top Performers rate some of those tools against the competition—evaluating what tactics they prefer and the top three tools they rated most effective. MRC members can benefit from using the Top Performers as a model for best practices in tool selection, fraud rate reduction and overall strategies and practices.

As eCommerce growth continues, effective fraud management strategies are increasingly relying on automation. The report concludes with a short Tips section designed to help guide MRC members as they move more of their fraud management processes into automation.

THE WORLD OF FRAUD MANAGEMENT



KEY TAKEAWAY 1

eCommerce fraud management is integral to business strategy, yet only 44% say it is extremely important to their business

- MRC members are more likely (54%) than general respondent organizations to consider eCommerce fraud management extremely important to their business strategy
- North American, Latin American, Middle Eastern and African businesses, enterprise-sized organizations and digital goods merchants are significantly more likely than most to feel this way

Many organizations still consider eCommerce fraud management to be a barrier to great customer service because it adds friction to the transaction process. With eCommerce sales continuing to grow, merchants are more aware than ever that they need to take eCommerce fraud management seriously, but fraud attack tactics are constantly changing, customers don't appreciate the extra steps during checkout, and a certain degree of online fraud is considered the cost of doing business. As a result, many merchants struggle to find the right balance for fraud within their overall business strategies.



I think [fraud management] is something that is typically not top of mind for the C-level unless they've experienced pain in the past.

ECOMMERCE DECISION MAKER
OFFICE SUPPLIES RETAILER, USA

I admit that, as a young company, we paid the price of inexperience, and we started putting solutions in place after a very serious incident we had when we started to sell in South Africa.

ECOMMERCE DECISION MAKER
APPAREL RETAILER, SPAIN

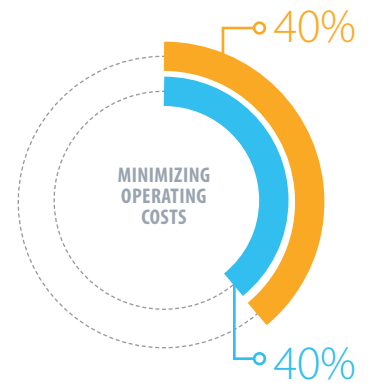
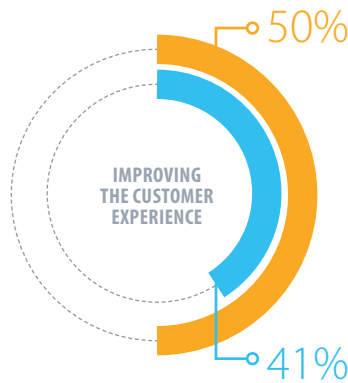
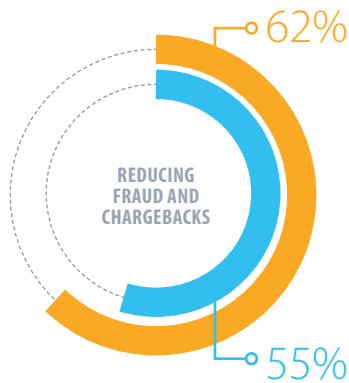
MRC members are more likely to rate all three pillars as extremely important compared to most organizations

When asked to choose which of the three pillars of the fraud management balancing act is most important, reducing fraud and chargebacks ranked first—with nearly half the vote (48%) across all groups regardless of region, size or vertical.

Overall, organizations are primarily focused on reducing fraud and chargebacks, with the other two pillars—improving the customer experience and minimizing operating costs—held as slightly less important.

PILLARS OF FRAUD MANAGEMENT

■ MRC MEMBERS ■ OVERALL



TOP PERFORMER INSIGHT

Top Performers are nearly **2.5x more likely to rate eCommerce fraud management as extremely important to their business strategy** compared to other organizations (83% vs. 35%). This suggests that the organizations that appreciate the importance of fraud management the most are the ones most likely to succeed at it.

KEY TAKEAWAY 2

Organizations who prioritize fraud management balance fare better against fraud—but these Top Performers make up only 18% of all merchants

North American (28%), Latin American (26%) and digital goods organizations (26%) are far more likely to be represented within this group.

Top Performers are statistically more likely than other organizations to strongly agree with the following statements about how their companies manage eCommerce fraud:

FRAUD MANAGEMENT CAPABILITIES IMPORTANT TO AGILITY

TOP PERFORMERS

OTHERS

Adapting fraud management to new business practices

68%

40%

Using data effectively

67%

39%

Identifying and mitigating risk from new fraud patterns

63%

36%

Testing and quantifying the impact of rule changes before going live

59%

33%

Adjusting rules without IT help

47%

18%

Managing fraud effectively can be a real struggle. Some organizations see effective fraud management as a barrier to good customer service, some underestimate its impact, some are simply new to eCommerce and others struggle to find the right tactics and tools.



The success rate of transactions and the fraud rate are kind of contradictory. If we're too strict, the success rate would decrease, and the customer experience will be worsened, while the fraud rate could be better controlled. If we're too loose on controlling fraud and include some risky transactions, then the customer experience could be obviously improved...The eventual goal is to achieve a dynamic balance of customer experience, success rate of transactions and fraud rate.

ECOMMERCE DECISION MAKER
AIRLINE, CHINA


Rising customer expectations are also impacting fraud management decisions. There is tension between strict fraud rules that help organizations minimize fraud loss and the desire to create a seamless eCommerce shopping experience.

Organizations are concerned that genuine customer orders may get rejected due to strict fraud rules and controls, which may result not only in the loss of that sale but also in the loss of a lifetime customer who is frustrated by the process.



TOP PERFORMER INSIGHT

Top Performers are more likely to have a broad range of fraud management capabilities, which gives them increased agility when responding to critical changes in the continually shifting fraud landscape.

 **TIP:** Organizational flexibility is very important when developing strong fraud management strategies. Fraud trends are constantly evolving and merchants must be willing to adapt to new technologies that can provide better insights and increase their ability to respond quickly in order to mitigate risks.

The average fraud chargeback rate for Top Performers is four times lower (0.1% vs. 0.4%) than other organizations.² This suggests that greater agility makes it possible for organizations to prioritize both a positive, minimal-friction customer experience and accurate and effective fraud detection and prevention. Organizations should make sure that their fraud management strategies are customer-centric and able to accept genuine orders automatically.

2. Self-reported

KEY TAKEAWAY 3

Responding to emerging attacks has been the top challenge over the past year—and most agree considerable room for improvement exists when it comes to using data to manage fraud effectively

FRAUD MANAGEMENT CHALLENGES

The biggest fraud management challenge today is responding to emerging fraud attacks, followed by updating fraud risk models, gaps in fraud tool functionalities, and omni-channel fraud. Fraud is always evolving—growing more prevalent and becoming faster and more sophisticated in response to eCommerce market expansion and better fraud management strategies.



TOP PERFORMER INSIGHT

Though identifying and responding to emerging attacks ranks as the #1 challenge across the board, Top Performers are statistically less likely to experience this challenge compared to others (38% vs. 46%).



As we develop new strategies and more sophisticated toolsets in the merchant realm to combat some of the more simple fraud... fraudsters are developing even more sophisticated toolsets and ways to get around our increased efforts. So, it's definitely... I really feel that it's changing.

FRAUD AND ORDER RESOLUTION DECISION MAKER
FINANCIAL SERVICES, USA

Unfortunately, [fraudsters] are always innovating. They have a lot of creativity for bad things—unlimited creativity. We see that the way we do things at some point becomes ineffective.

ECOMMERCE DECISION MAKER
ELECTRONICS AND RETAIL STORES, BRAZIL

IMPROVING DATA USE IN FRAUD MANAGEMENT

Nearly two-thirds of Top Performers (64%) say that there is a lot of room for improvement in how their companies should be using data to combat fraud. This is significantly higher than other organizations (55%).

- MRC members are on par with Top Performers in their prioritization of the need to improve data use (64%)
- All organizations agree that having disparate tools for different data streams is the top barrier to effective data use, closely followed by the big investments required to improve data use

Though merchants may not agree regarding the need to improve data use, they are all looking to improve analytics in the coming year, citing it as the #1 area for improvement, followed by improving automated detection accuracy, capturing and utilizing the right data, improving the chargeback dispute process, and creating mobile-specific fraud rules.



It's a constant cat and mouse game—there's no one solution, that would be absurd. There are very organized and specialized gangs that do this, and they know within a few days and check what measures you have implemented on the website or app.

ECOMMERCE DECISION MAKER
SPORTS AND APPAREL RETAILER, GERMANY



TOP PERFORMER INSIGHT

Top Performers are looking to improve both data use and analytics. This commitment to pushing their capabilities in both areas is a major reason why they sit ahead of the curve. **Improved analytics may help minimize false positives and manual interventions.**

High-quality, accurate data—combined with strong analytics—is essential for detecting patterns and trends which might indicate fraud.



TIP: Data is a key tool in the fight against fraud, but it is also important for understanding the consumer and maximizing their experience, especially for eCommerce-only retailers and service providers.

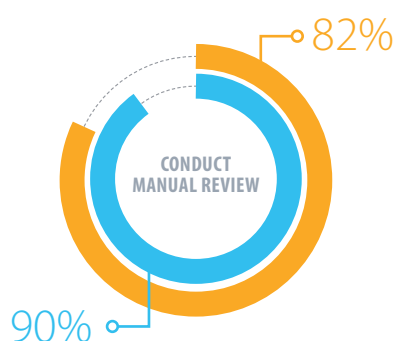
Data + Analytics =
A Winning Combination

KEY TAKEAWAY 4

Manual review remains essential, though it takes a toll on businesses, eating up 42% of fraud management budgets

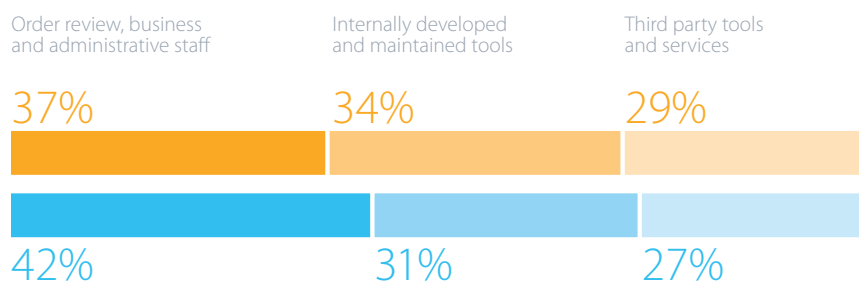
Fewer Top Performers engage in manual reviews compared to other businesses. Top Performers who do use manual review processes spend less on manual review (37%) compared to others (42%), preferring to devote a larger portion of their budgets to effective fraud management tools.

■ TOP PERFORMERS ■ ALL OTHERS



Base: North America, LAC, EUR, MEA and APAC
n= Top Performers – 347, All Others – 1623
D01. Please indicate the percent of eCommerce orders you manually screen for fraud.

PERCENT SHARE OF ECOMMERCE FRAUD MANAGEMENT SPENT ON...



Base: North America, LAC, EUR, MEA and Southeast Asia/Australia. Question not asked in North Asia, China, and India
n= Top Performers – 281, All Others – 1129
D05. Please indicate the percent of your current annual eCommerce fraud management spending that is allocated to each of the following areas.

MRC members have an opportunity for fraud screening improvements with a significantly higher post-review suspected fraud rate of 20%.

MRC members should work to improve their automated fraud screening to catch more suspected fraudulent transactions earlier and reduce the number of genuine transactions making it into manual review.

Top Performers who perform manual review report a post-review acceptance rate of 95%, on par with other organizations. While this means that post-review suspected fraud amounts to only 5%, it also suggests there is significant room for improvement in automated screening in order to reduce the number of valid transactions sent to manual review.

Most organizations recognize the need to improve automated detection accuracy in order to allow more genuine transactions to be approved before manual review—ranking it the 2nd-most important area in need of improvement.



TIP: Many Top Performers appear to put a greater focus on analytics and automated decision-making, reducing the time required per review, or eliminating the need for manual reviews altogether, suggesting a clear path forward for other merchants looking to reduce manual reviews and minimize operational costs.

KEY TAKEAWAY 5

Top fraud attacks will continue to evolve

96% of all eCommerce organizations report some form of fraud attack at their organization, with account takeover landing in the top three.

TOP 3 FRAUD ATTACKS EXPERIENCED



It's like having a physical store, but you're blind and deaf. You can't talk to your customers. You can't see them. So, all the information is in the data for everything eCommerce.

E-COMMERCE DECISION MAKER
GENERAL GOODS RETAILER, CANADA

COMBATING ACCOUNT TAKEOVER

Most organizations predict an increase in account takeover in the coming year, especially enterprise and digital goods organizations—reflecting a growing trend for consumers to store payment card details in online store accounts.

MRC members are statistically forward-thinking and vigilant regarding account takeover with 78% expecting account takeover attacks to increase compared to 59% of other organizations.

Account takeover fraud may be prevented by identifying suspicious account activity that signals a compromised account, before any purchases are attempted. In order to do this effectively, a fraud management solution should be able to:

- Challenge or block account actions based on monitoring of account creation, logins and updates
- Factor in data relating to usernames, passwords, addresses and devices used
- Take into account cross-merchant data
- Use account-monitoring results to inform fraud prevention rules for attempted purchases

KEY TAKEAWAY 6

Widespread dissatisfaction is driving desire to invest in additional tools

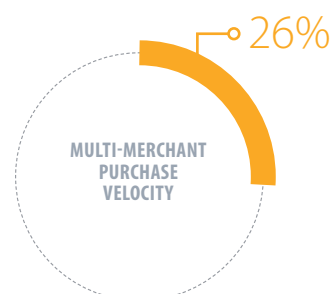
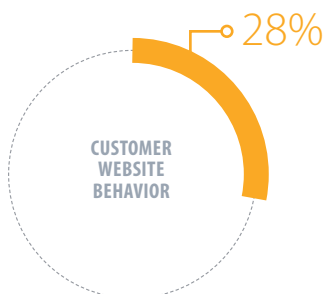
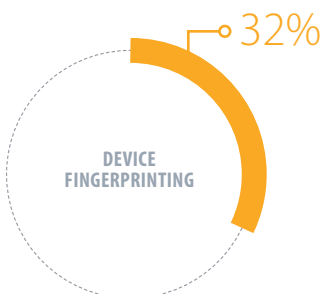
- Only 12% of all merchants are extremely satisfied with the tools available to them
- 21% of MRC members report extreme satisfaction
- 24% of Top Performers report extreme satisfaction
- North American, Latin American, Middle Eastern and African and enterprise organizations are all statistically more likely to fall into this category

Combining 'extremely' and 'very' satisfied groups reveals that 54% of companies are satisfied with the fraud management tools at their disposal, leaving a great deal of room for improvement. Even then, enterprise organizations are likely to feel that there is no one complete solution, while mid-market merchants often feel the available solutions are too complex.

Many merchants are interested in adding to their capabilities in the coming year, but the tools that most companies are interested in aren't considered very effective by the organizations already using those tools.

HIGH-INTEREST TOOLS WITH LOW EFFICACY RATINGS

■ % RATED EXTREMELY EFFECTIVE





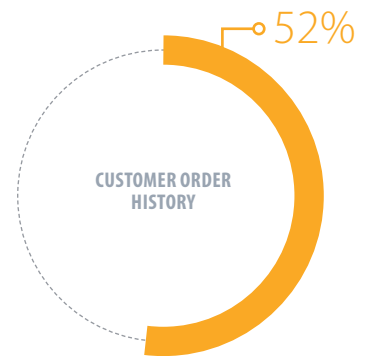
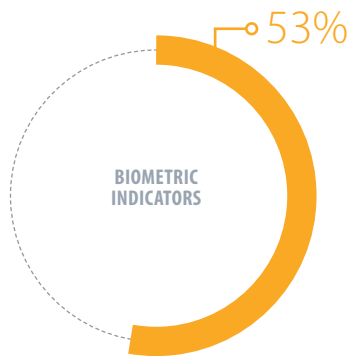
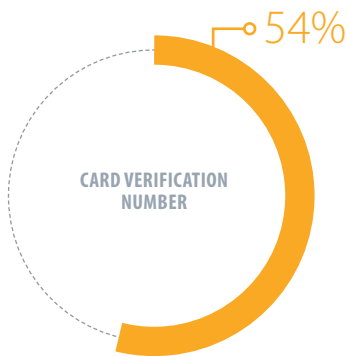
TOP PERFORMER INSIGHT

Top Performers find it less of a challenge to respond to emerging fraud attacks, and they enjoy a significantly wider range of fraud management capabilities, which gives them greater agility to respond dynamically to the constantly changing eCommerce landscape.

Top Performers should serve as a guide for those organizations looking to expand their toolsets in order to reduce fraud rates. Of their preferred tools, there were three that a relatively high percentage of Top Performers rated as extremely effective.

TOP PERFORMERS' EXTREMELY EFFECTIVE TOOLS

■ % RATED EXTREMELY EFFECTIVE



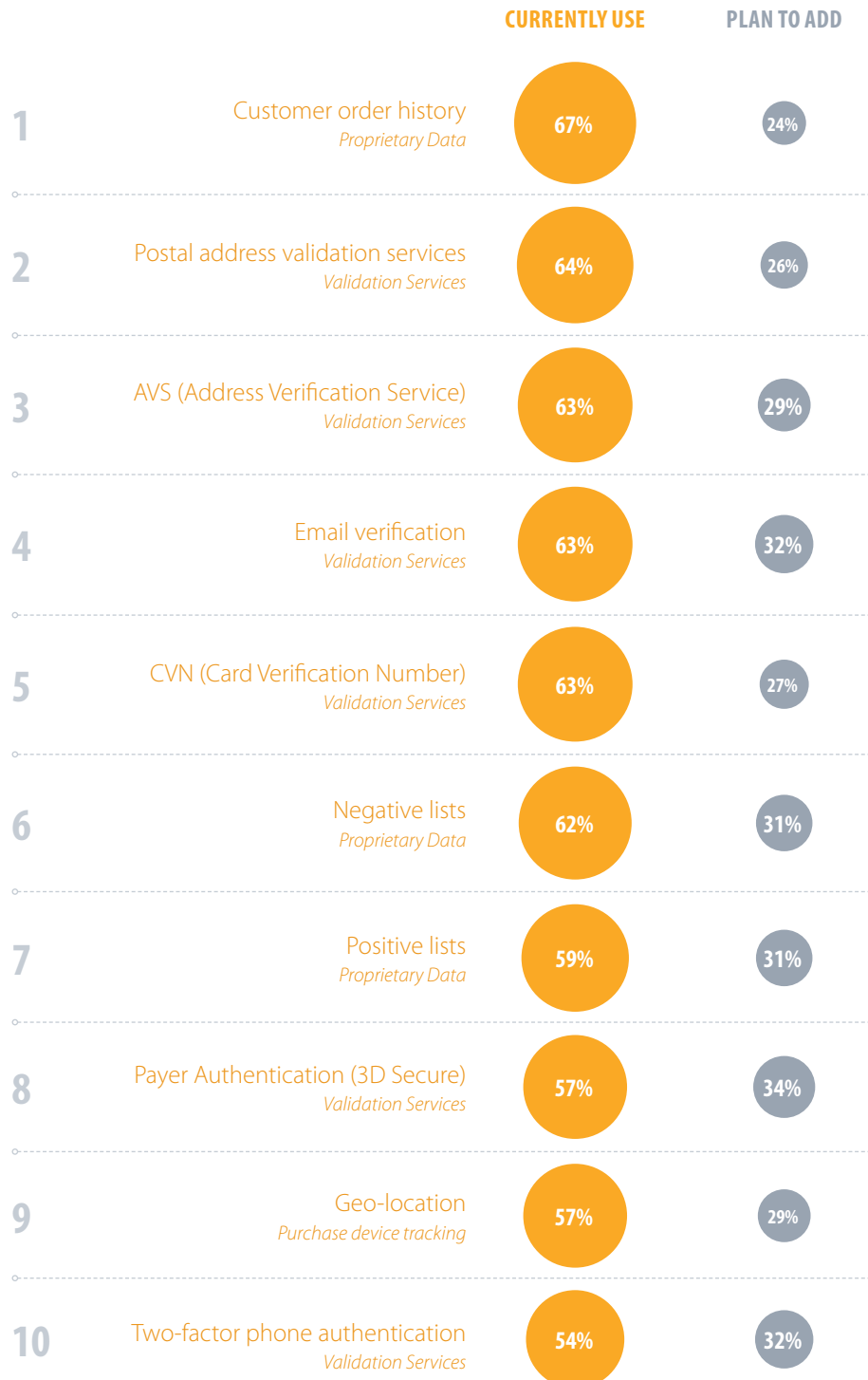
TOP PERFORMER INSIGHT

Top Performers note they are **more inclined to utilize the same tools across all channels** rather than taking an individualized, channel-specific approach compared to organizations with a higher fraud rate.

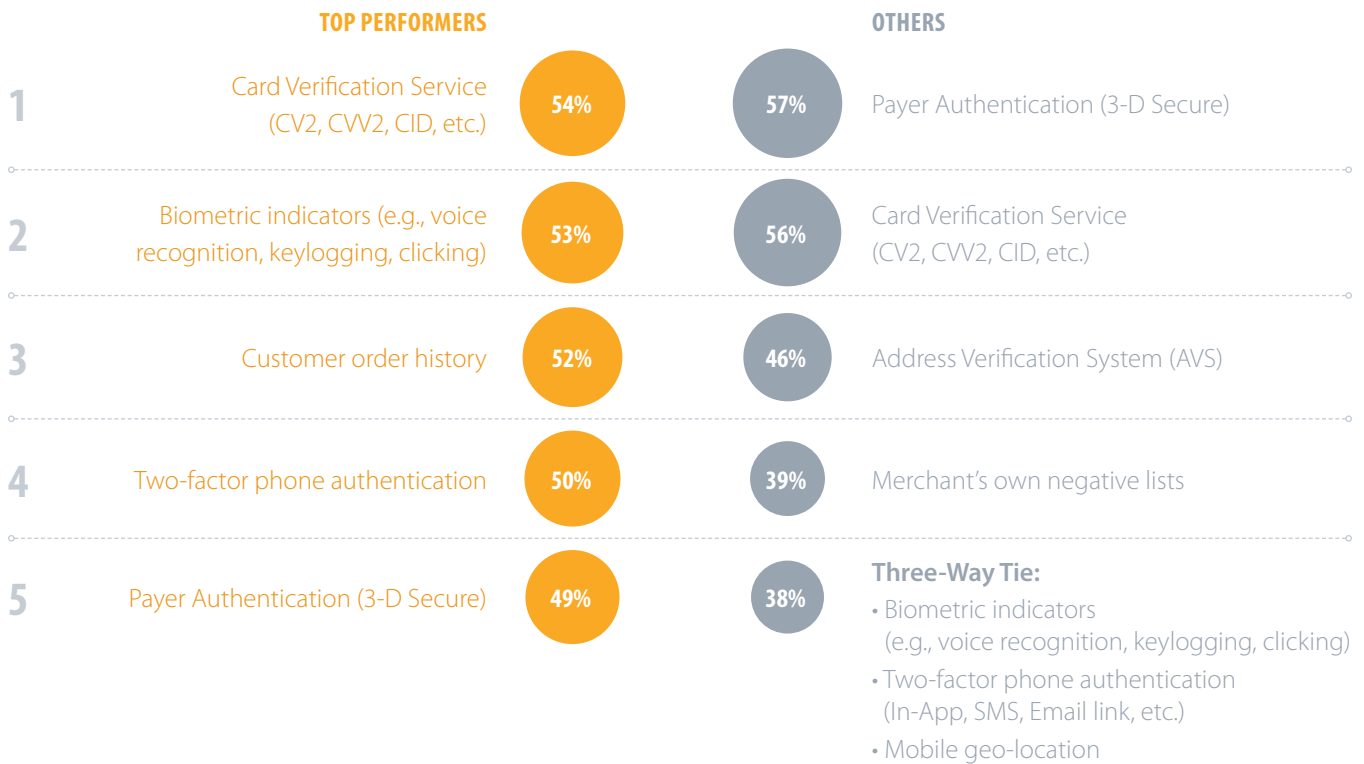
TOOLS ROUNDUP

Fraud Management Tools: An Overview

MRC MEMBERS' TOP TOOLS



MOST EFFECTIVE TOOLS



* Percentages are those in each group who use the tool and rate it as extremely effective.

** For further analysis of the differences between Top Performers' opinions and others' regarding the effectiveness of the full spectrum of fraud screening tools, see CyberSource's 2019 Global eCommerce Fraud Management Report.

Top Performers ranked AVS, merchant's own negative lists and mobile geo-location as relatively much less important than other merchants

Top Performers take a slightly different view of which tools are the most effective—particularly when it comes to customer order history—which they are nearly twice as likely to rate as extremely effective compared to other merchants (52% vs. 33%).

3-D SECURE

Both Top Performers and others ranked 3-D Secure (3DS) in their top five most effective tools. 3DS is one of the most-used tools in the fraud management toolkit, and thanks to the rollout of 3DS 2.0, 'better user experience' is now selected as the #1 benefit of using 3DS.

This popularity reflects the possibility that 3DS has become increasingly risk-based. Instead of challenging every transaction, issuers only challenge those shown to be a fraud risk through transaction risk analysis.

KPI GLOBAL OVERVIEW

	REGION				
	GLOBAL	NORTH AMERICA	LATIN AMERICA	ASIA-PACIFIC	EUROPE
% of annual eCommerce revenue lost due to payment fraud on domestic orders	1.6	1.5	1.3	1.5	1.9
% of domestic eCommerce orders rejected due to suspicion of fraud	2.5	3	2.8	2	3
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.3	0.7	0.6	0.1	0.7
% of eCommerce orders manually screened for fraud	25	16	20	30	20
% of eCommerce orders declined after manual review	3	10	20	1	10

	ECOMMERCE REVENUE			VERTICALS				
	SMALL	MID-MARKET	ENTERPRISE	PHYSICAL GOODS	DIGITAL GOODS	SERVICES	FOOD, GROCERY, RESTAURANT AND QSR	TRAVEL
% of annual eCommerce revenue lost due to payment fraud on domestic orders	1.5	1.6	1.7	1.8	1	1.6	2.8	1.2
% of domestic eCommerce orders rejected due to suspicion of fraud	2.7	2.4	2.5	2.6	2.5	2.1	3	2
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.5	0.2	0.4	0.4	0.4	0.2	0.1	0.3
% of eCommerce orders manually screened for fraud	30	25	20	25	30	30	15	27
% of eCommerce orders declined after manual review	5	2.5	3	4	2	2	4	2

Note: Medians are shown for all KPIs

Disclaimer: The results in the 2019 Global eCommerce Fraud Management Report are not recommended for year on year comparisons with previous regional CyberSource eCommerce Fraud Management reports. The sample in the 2019 global survey includes a different sample methodology, one which has been developed to give a more holistic picture of fraud today at a global level.

In partnership with

CyberSource®
A Visa Solution

Global Fraud Survey Results 2019 | 19

MRC Building
Better Commerce
Fraud & Payments Professionals

CONCLUSION

Top Performers appear to look at fraud management from a different perspective than other merchants, which leads them to value a slightly different set of tools as more important and more effective. Their preferred tools show that Top Performers tend to rely more heavily on analytics and automation, which allows them to spend less time and money on manual reviews, while still keeping their chargeback rates low.

As eCommerce volume continues to grow, manual review processes can quickly be overwhelmed without increased analytics and automation support. As a result, more merchants will consider adding tools that rely on automation to help manage and minimize fraud, while also controlling operational costs and supporting an improved customer experience.

LEARN MORE

For more detailed regional perspectives on fraud management, please email sales@cybersource.com.

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

TIPS FOR EFFECTIVE FRAUD MANAGEMENT AUTOMATION

- ✓ Use an array of effective tools, including: validation services, proprietary data, multi-merchant data and purchase device tracing
- ✓ Maintain positive and negative lists to allow seamless processing of known genuine customers and automatic filtering of known fraudsters
- ✓ Create customer-centric rules to allow genuine customers to pass through unaffected—ensuring that these rules are continually reviewed and recalibrated
- ✓ Streamline the review process by using an effective case management system that brings together all the tools reviewers need to review orders efficiently
- ✓ Ensure a feedback loop so that insights from the review team can be fed into machine learning automation, rules and positive/negative lists

JOIN MRC

The Merchant Risk Council is dedicated to building the definitive library of eCommerce best practices, creating a robust collection of resources for members to draw on as they continue to fine-tune their own strategies and toolsets. MRC merchants benefit from sharing their own best practices in fraud management with their MRC peers. MRC merchants are knowledgeable, informed and know they can continuously improve by implementing the right tools and efficiencies to keep fraud in check. If you are interested in joining MRC, visit merchantriskcouncil.org/about-mrc/contact-us to fill out an application form.

METHODOLOGY

The survey subjects represent 34 countries across North America, Latin America, Europe, the Middle East, Africa and Asia-Pacific. The quantitative survey was primarily conducted in April, May and June of 2018. For Southeast Asia and Australia, it was conducted in October and November of 2017. Qualitative interviews were commissioned afterward to explore influencers' and decision makers' opinions on the quantitative results. A sampling quota was used, with the number of respondents by region benchmarked against eCommerce volume by region.³

The MRC would like to thank the participants for taking the time to complete the online survey, CyberSource for developing the survey and providing analysis and GfK for performing the survey. If you are interested in discussing any of these fraud-related findings and their implications, the MRC will be pleased to organize a follow-up conversation to talk about the results in further detail.

RESPONDENT ROLES

Quantitative: 2,769 respondents comprising those who:

- Make or influence eCommerce fraud management decisions: 49%
- Are involved in eCommerce fraud management: 51%
- Of these, 256 were MRC members; 60% of MRC member respondents have online revenue of more than \$25M

Qualitative: 49 fraud management decision-makers, across 15 markets, participated in post-quantitative interviews

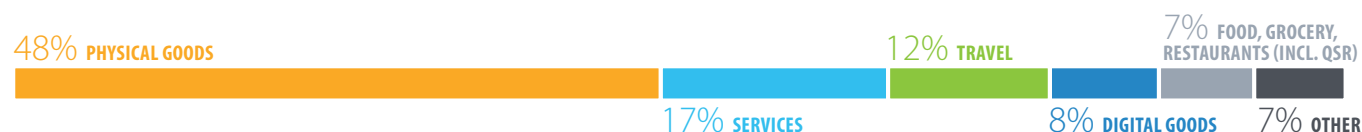
GEOGRAPHICAL DISTRIBUTION OF REVENUE REPRESENTATION⁴



SIZE OF BUSINESS BY ANNUAL ECOMMERCE REVENUE¹¹



MARKET SECTORS¹¹



3. Euromonitor

4. Due to rounding, percentages may not always appear to add up to 100%.



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

In partnership with

CyberSource®
A Visa Solution

