Masters of Balance

What it takes to be a fraud management leader

2019 Global eCommerce Fraud Management Report

CyberSource®
A Visa Solution

Contents

What do the colors mean?

As you read the report, you'll see some results in gold and others in blue.

The results in gold refer to those organizations that place equal importance on maximizing revenue, minimizing fraud loss and minimizing operational costs.

The results in blue refer to those organizations that don't.

And be sure to pay close attention to results with a green star. They highlight the statistically significant results, and some of the most valuable insights in this report.

LEADERS

OTHERS

STATISTICALLY SIGNIFICANT ★

Throughout this report, 'eCommerce' covers the sales of products and services ordered or booked online, using any device (with mCommerce regarded as a subset of eCommerce).

Executive summary

This global report[1] captures the views of nearly 2,800 fraud management specialists, representing organizations across 34 countries.

Offering key insights and tips, it examines the characteristics of those organizations that place equal importance on all three areas of the fraud management balancing act:

- Delivering a positive experience for genuine customers and maximizing the acceptance of genuine orders
- Accurately detecting and rejecting fraudulent orders to minimize fraud losses
- Efficiently managing the operational costs of fraud management activities

When we compare those that place equal attention on all three aspects—those that appear to have mastered balance—to those that don't, we see statistically significant differences that mark the former as **leaders**.

The survey reveals a number of statistically significant differences between those that prioritize balance, a group we are calling the leaders, and those that don't, the rest of the respondents.

[1] All of the respondents either make or influence decisions about eCommerce fraud management, or are directly involved in it. They represent organizations of all sizes from five verticals and 34 countries across North America, Latin America, Europe, the Middle East, Africa and Asia Pacific. See the end of the report for details of the survey
[2] Results are self-reported by survey respondents

Just 18% of the respondents are categorized as **leaders**. They:

1

Have a chargeback rate **four times lower** than the other respondents[2]

LEADERS 0.1%
OTHERS 0.4%

2

Are **2.5x more likely** to rate eCommerce fraud management as extremely important to their organization's business strategy

LEADERS 83%
OTHERS 35%

3

Find it less of a challenge to respond to emerging fraud attacks

LEADERS 38%
OTHERS 46%

4

Have a significantly greater range of capabilities that give them agility to respond to the dynamic landscape they operate in

5

Have a greater capability to use data effectively for fraud management

LEADERS 67%
OTHERS 39%

6

Are less likely to conduct manual review…

LEADERS 82%
OTHERS 90%

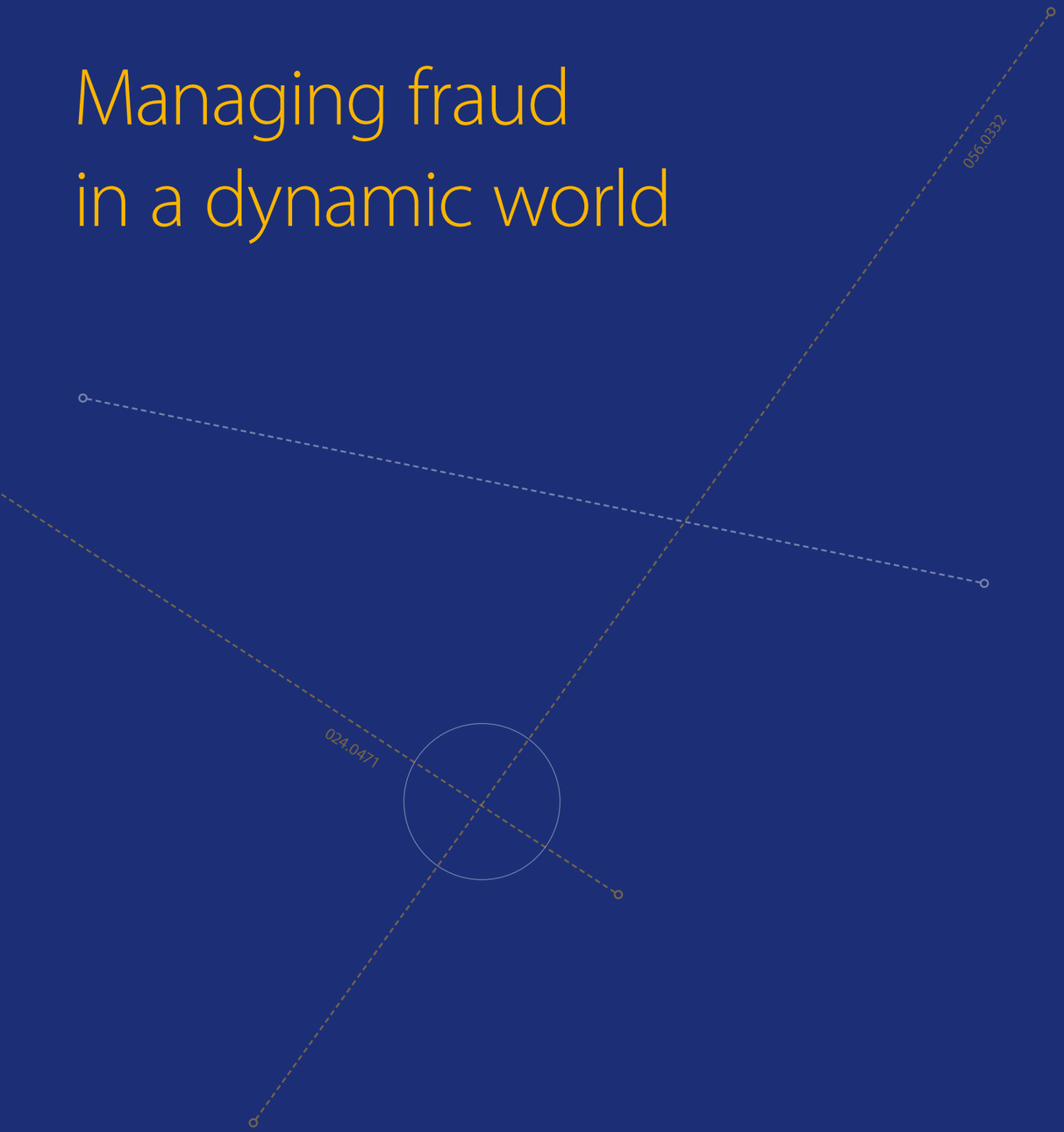
…and spend less in this area

Leaders allocate less of their annual eCommerce fraud management budget to order review staff

LEADERS 37%
OTHERS 42%

In this report, we'll explore these differences, and offer insights and tips to help your organization move forward with its own fraud management strategies and practices.

Managing fraud in a dynamic world



Consumer expectations are increasingly being set by masters of digital commerce, such as:

Retailers that offer in-store pick-up within an hour of purchase

Restaurants that let them use a voice-activated device in the home to order takeout

Taxi companies they can hail and pay for directly from the chat app they're using

It's not just digitally native organizations that are raising the bar. Traditional businesses are also getting better at delivering convenient, personalized and integrated customer experiences that cross digital and physical boundaries.

As they invest and immerse themselves in digital transformation, organizations have to make every sale count. Falling short of conversion due to a poor fraud management decision is not an option. The cost is not only that revenue, but potentially any further revenue from that customer.

Customer-centric fraud management

Strict fraud rules and controls could mean that genuine customer orders are flagged as fraudulent, resulting in a negative experience for that customer. Beyond the loss of revenue from a single sale is a larger concern: that customers may be lost for good, as well as the potential revenue they could bring.

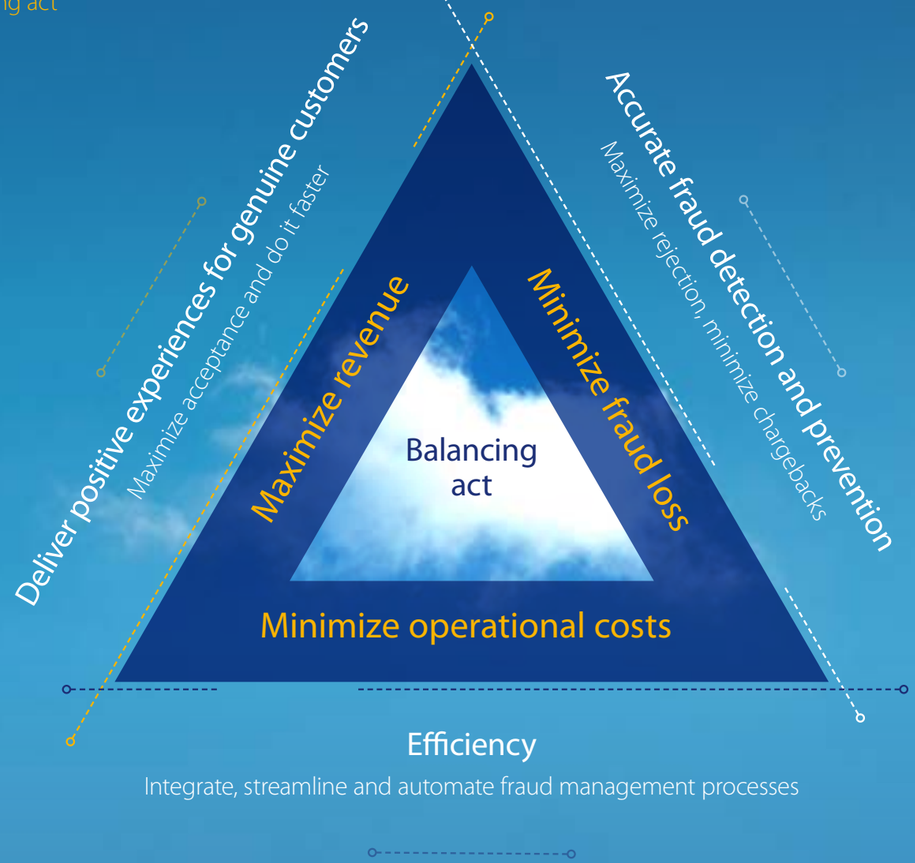
In addition, a negative experience may be shared by word of mouth or on social forums where multiple existing and/or potential new customers reside, affecting a brand's reputation.

An effective fraud management strategy should be customer-centric, where the focus is on ensuring that genuine customer orders are automatically accepted.

Lead with balance

Effective fraud management requires the careful balance of three interdependent dimensions.

Figure 1.
The fraud management balancing act



Customer and fraudster behaviors are continually adapting to developments in technology, culture and economics. Fraud management objectives and budgets change with evolving business realities.

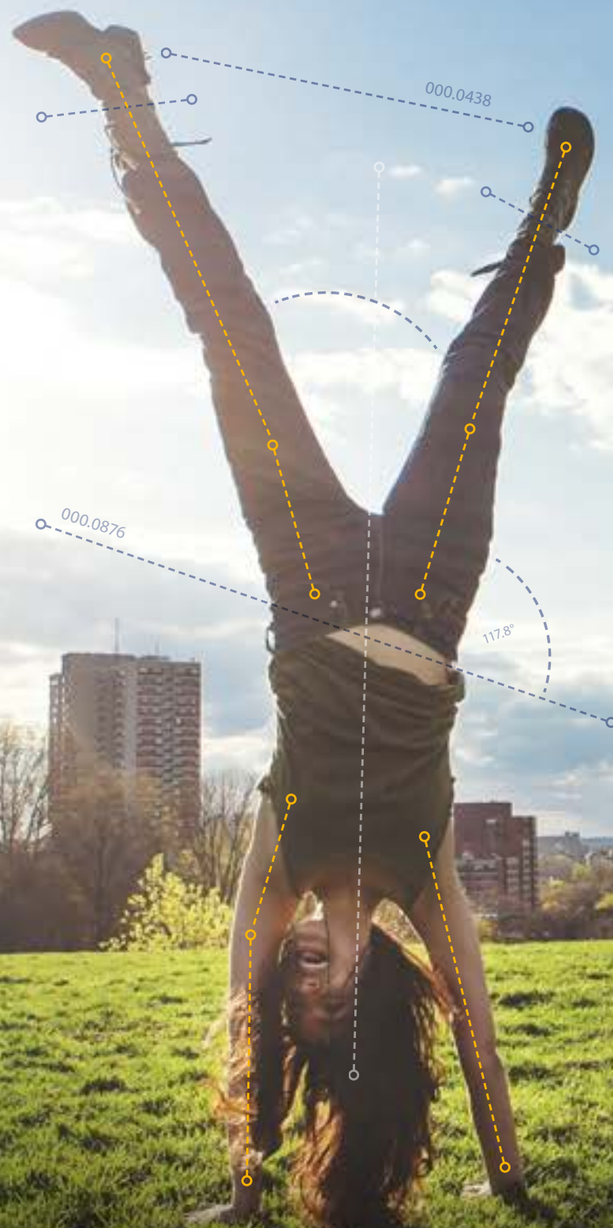
In this dynamic landscape, it takes constant recalibration and fine-tuning of fraud management controls and processes to keep achieving the best balance.

Calibrate, review, recalibrate

The optimal point of balance is unique to each business. This is why a 'set it and forget it' approach to fraud management won't deliver the best results. It will not, for example, let you treat specific SKUs differently, or adapt to short-term events that cause normal customer behavior to temporarily change, such as a promotion or holiday season.

Choose an approach that gives you fine-tuning flexibility along with sophistication in responding to changing fraud trends. For optimal results, a fraud solution should be able to:

- Use machine learning to keep pace with macro shifts in fraud trends by detecting patterns in large data sets
- Supplement this with flexible rule-setting for precision control and adaptability to specific influencing factors
- Leverage advanced machine learning techniques to suggest rules, based on your own historical data, that are likely to help you achieve your fraud management objectives



> "The acceptance rate of transactions and the fraud rate are contradictory.
>
> If we're too strict with our fraud management rules, the acceptance rate would decrease and this could affect the customer experience, but the fraud rate would be lower. If we're too relaxed on fraud management rules and accept some risky transactions, the customer experience could be obviously improved. The ultimate goal is to achieve a dynamic balance of customer experience, acceptance rate of transactions and fraud rate.[3]
>
> **Role:** eCommerce Decision Maker | **Vertical:** Travel | **Country:** China

[3] This quote has been translated from Chinese to English

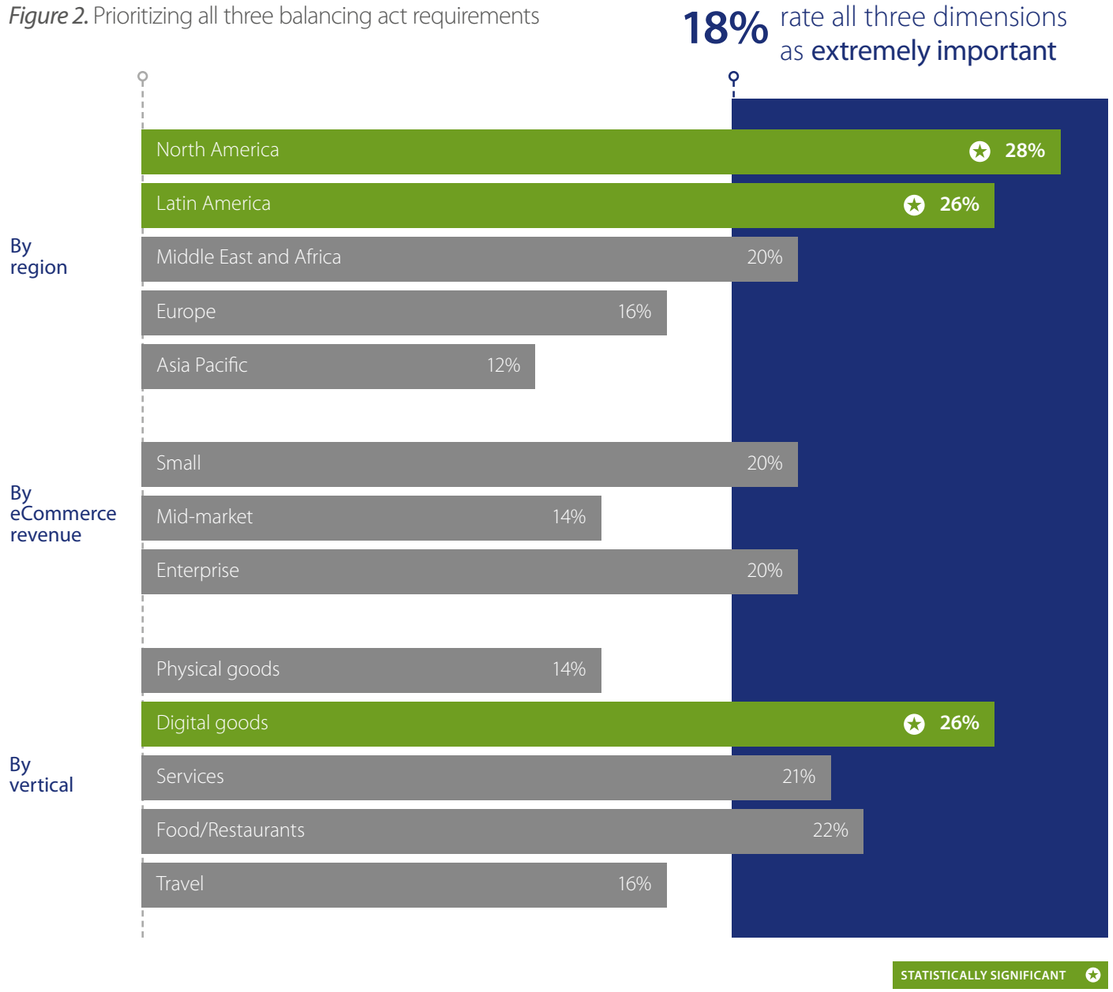
The masters of balance

Asked to rate the importance of each dimension of the balancing act, only 18% of respondents—fewer than one-fifth—gave all three the highest priority.

North American and Latin American organizations, and those offering digital goods, are the most likely to prioritize balance.

When we compare those that place equal attention on all three aspects of the balancing act—those that appear to have mastered balance—to those that don't, we see significant differences in six key areas that mark the former as leaders.

Figure 2. Prioritizing all three balancing act requirements



Base 1970 (Question not asked in South East Asia and Australia)
Question: 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
Answer options: Extremely important, very important, somewhat important, not very important, not at all important

Six characteristics of the masters of balance

The survey reveals a number of statistically significant differences between those that prioritize balance and those that don't.

Masters of balance:

1. Have a chargeback rate **four times lower** than the other respondents
2. Are **2.5x more likely** to rate eCommerce fraud management as extremely important to their organization's business strategy
3. Find it less of a challenge to respond to emerging fraud attacks
4. Have a significantly greater range of capabilities that give them agility to respond to the dynamic landscape they operate in
5. Have a greater capability to use data effectively for fraud management
6. Are less likely to conduct manual review, and spend less in this area

1 Lower chargeback rate

The average fraud chargeback rate of leaders is four times lower than that of the others in the survey (0.1% vs 0.4%). This shows that it's feasible to pursue both a better customer experience and lower fraud losses.[4]

2 More likely to consider fraud management as strategic

Leaders were almost 2.5 times more likely than the rest to say that eCommerce fraud management is extremely important to their organization's business strategy.

When organizations appreciate the significance of fraud management to their business success, they appear to do better at it.

Figure 3. Strategic importance of fraud management

Base 1970 (Question not asked in South East Asia and Australia)
Question: How important is eCommerce fraud management to your organization's business strategy?
Answer options: Extremely important, very important, somewhat important, not very important, not at all important

> [eCommerce fraud] It's extremely important to our business...
>
> I would say, four years ago or even five years ago, because the amounts were not material enough for us to jump in and do something, we just accepted that risk as, okay, fine, we lose a little bit of money, but it's nothing to worry about, kind of thing. And then, we saw it quadruple within the next year and then again double within the following year. So, third year, we are looking at huge amounts, and then it's like, okay, now we need to take this seriously and get something done about it.
>
> **Role:** Finance Decision Maker | **Vertical:** Travel | **Country:** Canada

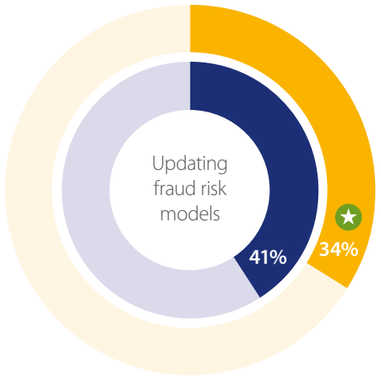
[4] Results are self-reported by survey respondents

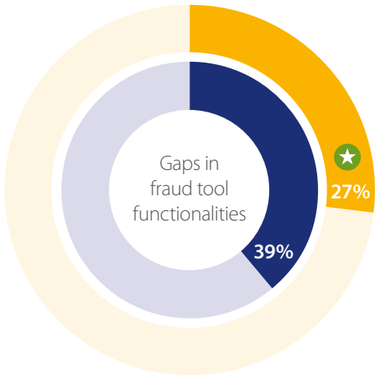
3 Less challenged by emerging fraud attacks

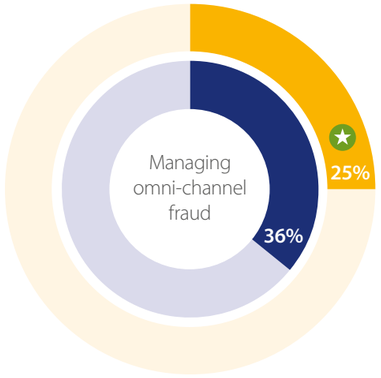
The biggest fraud management challenge today is responding to emerging fraud attacks. This makes sense given the growing sophistication of fraudsters and their speed in exploiting new vulnerabilities.

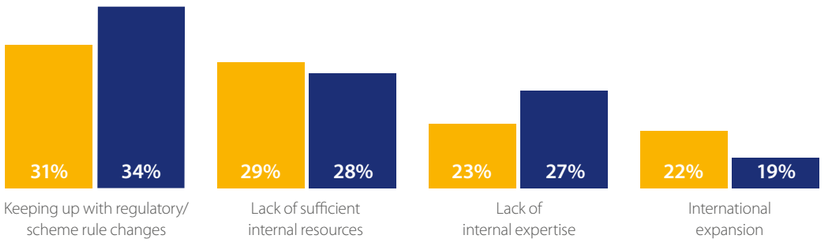
However, leaders experience this challenge—along with almost all other fraud management challenges—less than the other respondents do.

Figure 4. Fraud management challenges
(% experiencing the challenge in the previous year)









LEADERS
OTHERS
STATISTICALLY SIGNIFICANT

Leaders experience these four fraud management challenges significantly less than others

Base 1410 (Question not asked in South East Asia and Australia)
Question: Which of the following challenges related to eCommerce fraud management, if any, have you experienced in the last 12 months?

Keep pace with evolving fraud

Advanced machine learning techniques, that leverage massive breadth and depth of data, can considerably ease the challenge of identifying and responding to emerging attacks.

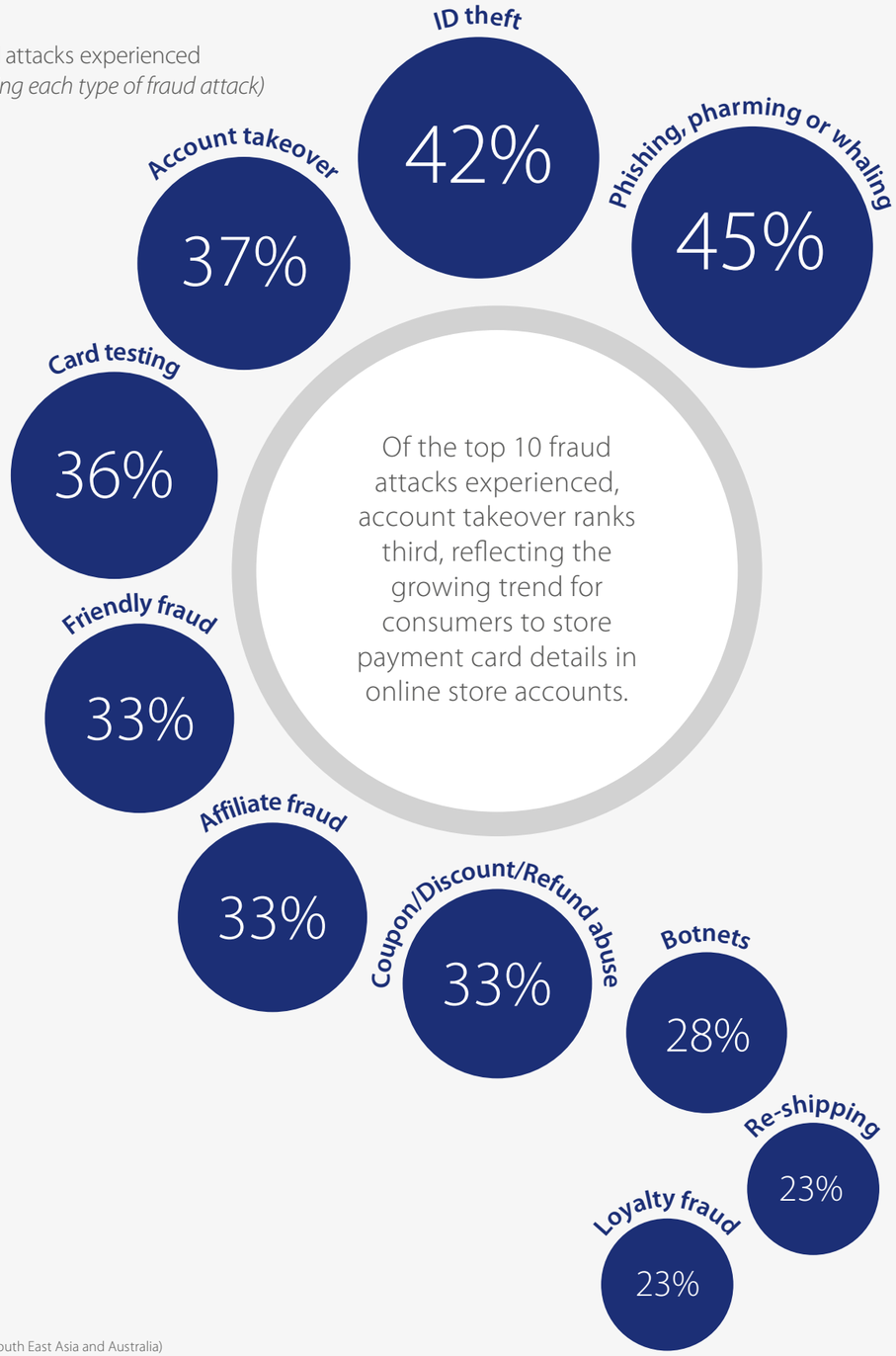
A sophisticated fraud management solution that combines static and self-learning models will analyze and process new data, autonomously updating its models to reflect the latest trends, leaving you to focus your efforts on ensuring that genuine customers aren't turned away.

Static models learn how to identify fraud at a point in time by sifting through millions of transactions. They are very effective at identifying historical fraud patterns.

Self-learning models incorporate data from new transactions to recognize and adapt to ever-evolving fraud patterns. Self-learning models are effective at identifying the latest fraud tactics.

Taking on account takeover

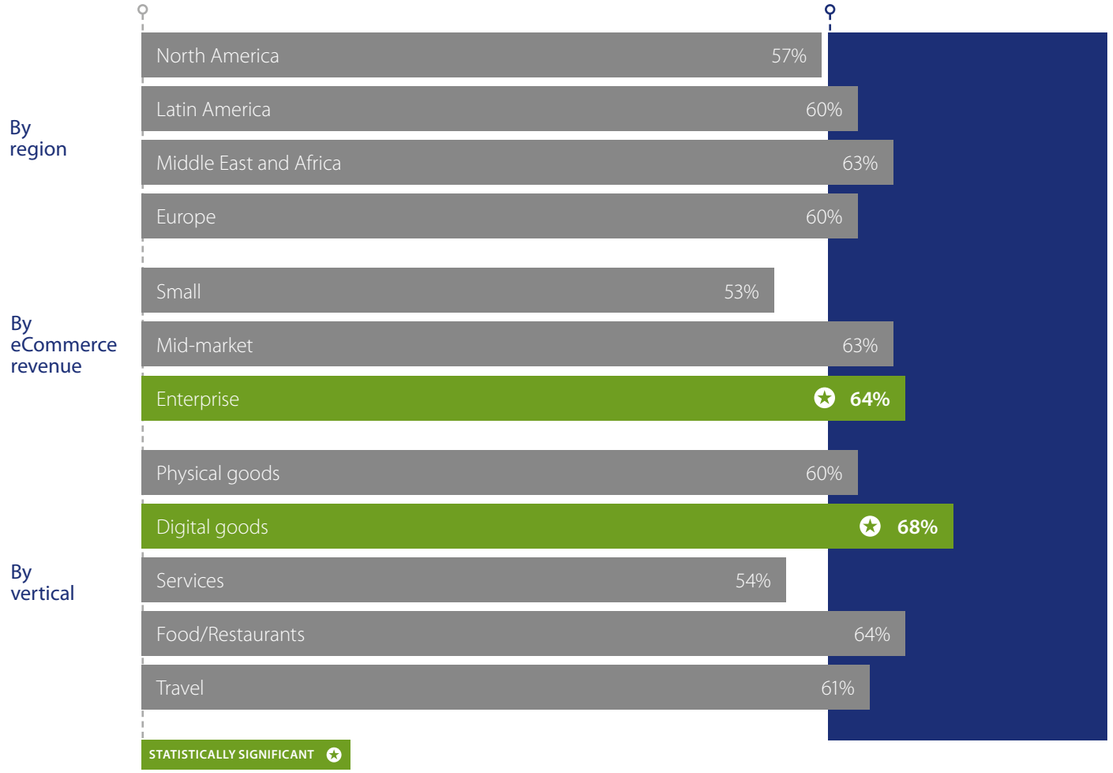
Figure 5. Top 10 fraud attacks experienced
(% experiencing each type of fraud attack)



Base 1970 (Question not asked in South East Asia and Australia)
Question: Which of the following types of fraud attacks, if any, have you ever experienced at your company?

59% of respondents anticipate that account takeover attacks will increase in the next 12 months

Figure 6. Account takeover expected to rise



Enterprise level organizations and those in the digital goods vertical are the most likely to expect an increase in account takeover in the coming year

Addressing account takeover

Fraud perpetrated through account takeover can be prevented by detecting suspicious account activity before a compromised account is used to attempt a purchase.

To do this, 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

Base 1410 (Question not asked in South East Asia and Australia) **Question:** Over the next 12 months, do you see account takeover…
Answer options: Increasing a lot, increasing a little, staying about the same, decreasing a little, decreasing a lot?

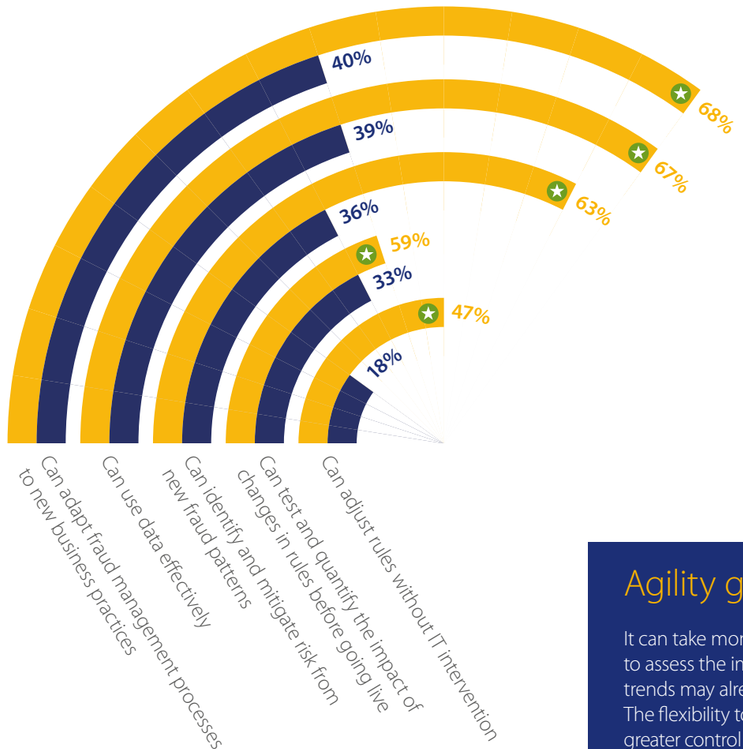
4 Leading in fraud management capabilities

Leaders are more likely to have a range of fraud management capabilities that give them the agility to respond to the continually shifting landscape in which they operate.

These include the ability to adapt fraud management processes and rules, to identify and mitigate risk from new fraud patterns, and to use data effectivelyto manage fraud.

Significantly more leaders strongly agree that their organizations do the following five things.

Figure 7. Fraud management capabilities important to agility



Agility gives stability

It can take months to gather enough chargeback data to assess the impact of rule changes. By then, fraud trends may already have shifted or further evolved. The flexibility to fine-tune rules helps to provide greater control over fraud management strategies.

An agile fraud solution is one that can:

- Perform 'what if' analyses to test any rule on the business historical transaction data
- Assess the likely impact of proposed rules before being deployed in a live environment

Base 1970 (Question not asked in South East Asia and Australia)
Question: Please indicate the extent to which you agree or disagree with each of the following statements about how your company manages eCommerce fraud
Answer options: Strongly agree, somewhat agree, somewhat disagree, strongly disagree

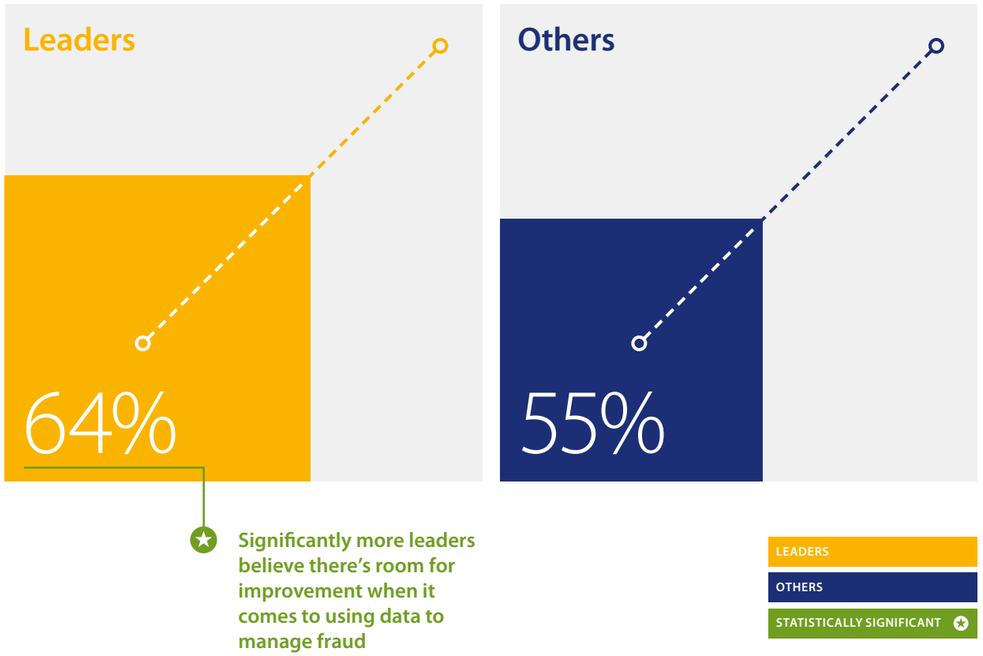
5 Use data in a more effective manner

Leaders have a greater capability to use data effectively for fraud management (**67% vs 39%**, as shown in *Figure 7*).

When asked how much room for improvement they see in their organization's use of data to manage fraud, almost two-thirds of the leaders (**64%**) believe there's a lot of room for improvement, compared with just over half (**55%**) of the other respondents.

This suggests that the more effective organizations are at using data, the more they see the advantages and want to exploit these advantages even further.

Figure 8. Room for improvement in data use for fraud management

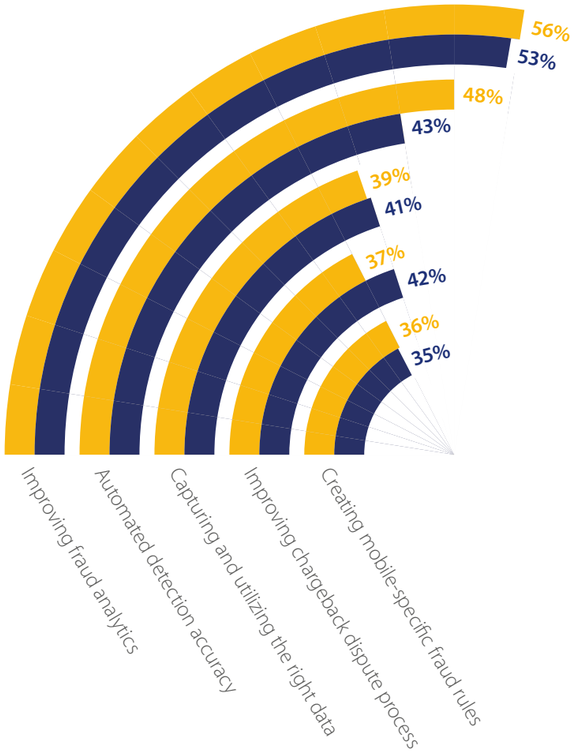


Significantly more leaders believe there's room for improvement when it comes to using data to manage fraud

Base 1410 (Question not asked in South East Asia and Australia)
Question: How much room for improvement do you see in how your company should be using data to manage fraud?
Answer options: A lot, a little, none at all

Asked to indicate which of eight options are areas for improvement for their organization over the next year, both the leaders and the rest selected three data-centric options among their top five.

Figure 9. Top five areas for improvement in the next year
(% selecting the option)



LEADERS
OTHERS

Base 1410 (Question not asked in South East Asia and Australia)
Question: Thinking ahead to the next 12 months, which of the following, if any, are areas for improvement for your organization?
Answer options: Automated detection accuracy, streamlining manual review tasks and workflow, improving fraud analytics, creating mobile specific fraud rules, better managing of omni-channel fraud, improving chargeback disputes process, outsourcing portions of the review/screening operation, capturing and utilizing the right data, other

In interviews, many fraud managers acknowledged that fraud management tools and strategies can only work if the data that is fed into them is accurate and of high quality.

Enterprise organizations are looking for tools to help with analyzing and reporting on existing data sources, whereas mid-sized organizations are more focused on access to more data to supplement what they already have.

6 Less likely to conduct manual review

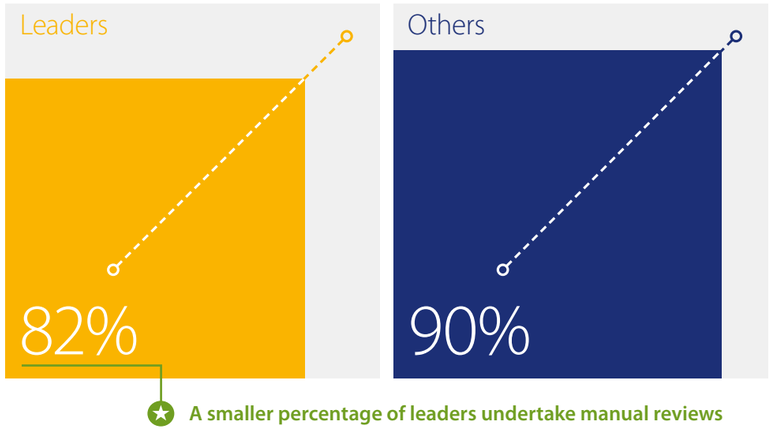
Almost all of the respondents review orders manually but significantly fewer of the leaders perform manual reviews compared to others **(82% vs 90%)**.

The leaders also:

- Spend a lower proportion of their eCommerce fraud management budget on review—spending relatively more on effective use of fraud management tools (*Figure 11*)
- Take less time on average to review an order (10 vs 15 minutes for everyone else)

All this suggests that leaders have a greater focus on analytics and automated decision-making.

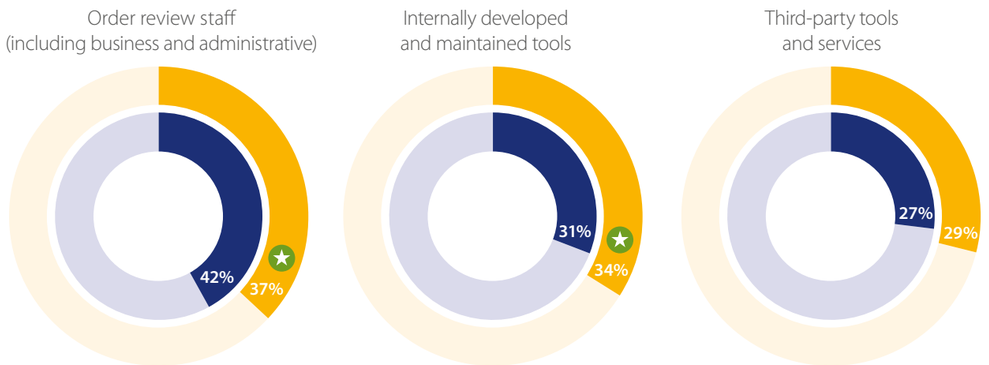
Figure 10. Most respondents conduct manual reviews
(% of respondents conducting manual review)



LEADERS
OTHERS
STATISTICALLY SIGNIFICANT

Base 1970
Question: Please indicate the percent of eCommerce orders you manually screen for fraud
Note: The figure takes the number of each group that answered 'None—we do not conduct any manual reviews' and subtracts it from 100

Figure 11. Split of eCommerce fraud management budget



Base 1970
Question: Please indicate the percent of your current annual eCommerce fraud management spending that is allocated to each of the following areas

Five tips for effective fraud management automation

Over-reliance on manual review becomes less viable as eCommerce volumes grow.

As you look to automate more decision-making, follow these tips:

1

Use an array of effective fraud management tools that include validation services, proprietary data, multi-merchant data, and purchase-device tracing

2

Maintain positive and negative lists to allow seamless processing of known genuine customers, and automatic filtering of known fraudsters

3

Create customer-centric rules to allow genuine customers to pass through unaffected—ensuring that these rules are continually reviewed and recalibrated

4

Streamline the review process by using an effective case management system that brings together all the tools reviewers need to review orders efficiently

5

Ensure that there is a feedback loop so that insights from the review team can be fed into your automation rules and positive/ negative lists

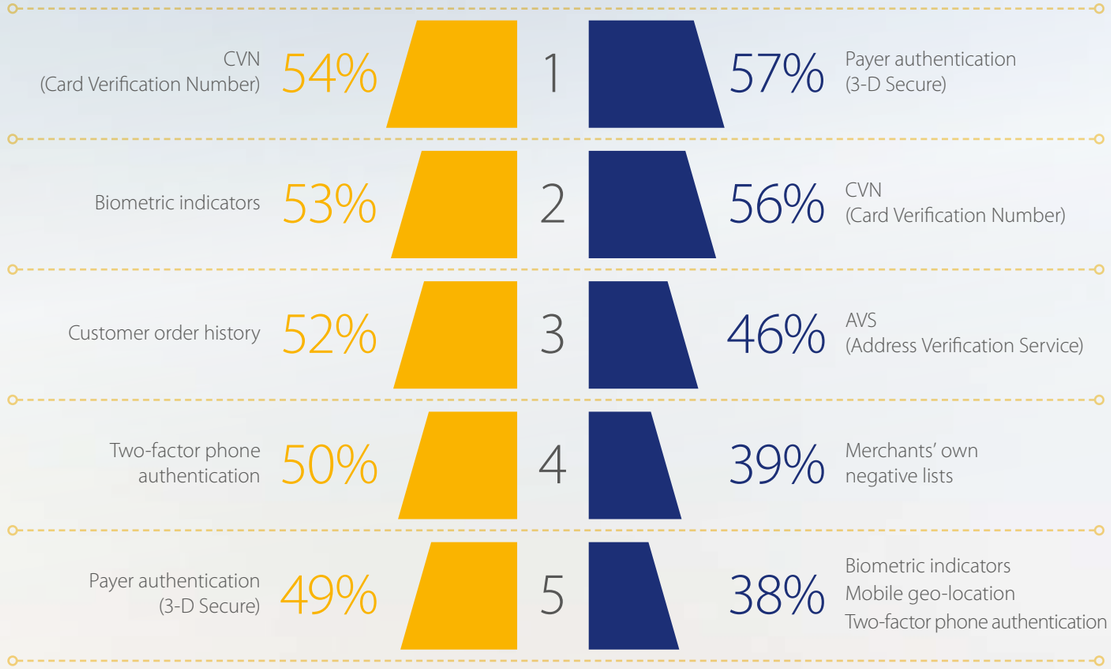
When interviewed, fraud managers anticipate that machine learning and AI will increasingly take on more of the manual review process, and that manual review will evolve to focus on the most complex and difficult cases.

The effectiveness of fraud screening tools

All the respondents use the same range of tools to help detect fraud, but the leaders have a slightly different view of which tools are the most effective. There are half a dozen tools where there's a big difference in effectiveness rating between the leaders and others.

This points to the leaders making different strategic and practical use of key tools, which may account for how they are able to achieve their position of leadership with the same toolkit.

Figure 12. Most effective tools[5]
(% rating tool as extremely effective)



Most effective tools

Looking at the tools rated as 'extremely effective' by the respondents, the five most effective for the leaders and the others are similar but not identical.

Address Verification Service (AVS), merchants' own negative lists and mobile geo-location are relatively much less important to the leaders than to the other respondents:

- AVS: tied 18th for leaders (38%); 3rd for others (46%)
- Negative lists: 10th for leaders (44%); 4th for others (39%)
- Mobile geo-location: 20th for leaders (37%); tied 5th for others (38%)

LEADERS

OTHERS

Base 1147 (Question asked in North America and Europe only)
Prioritize balance (n=219),
Do not prioritize balance (n=928)
Question: How effective are each of the following tools in detecting eCommerce payment fraud?

[5] Percentages are those in each group that use the tool and rate it as extremely effective

Differences in perceived effectiveness

The significant outlier in the top five is customer order history. This is one of the tools that leaders find significantly more effective at detecting eCommerce payment fraud than the other respondents do. These tools include:

- Search engine results (leaders 43% vs others 18%)
- Order velocity monitoring (45% vs 23%)
- Identity morphing models (43% vs 21%)
- Customer order history (52% vs 33%)
- Fraud scoring model: company specific (45% vs 26%)
- Credit history check (46% vs 28%)

These tools come from three of the four tool categories—validation services, proprietary data sources, and multi-merchant data sources—showing that leaders understand the value of using a breadth of different data sources to manage fraud effectively.

Figure 13. Effectiveness of tools among those who use them
(% rating tool as extremely effective)

		Users that prioritize balance	Users that do not prioritize balance
Validation services	CVN (Card Verification Number)	54%	56%
	Biometric indicators	53%	38%
	Two-factor phone authentication	50%	38%
	Payer authentication (3-D Secure)	49%	57%
	Credit history check	46%	28%
	Search engine results	43%	18%
	Postal address validation services	43%	29%
	Paid-for public records services	42%	27%
	Email verification	41%	24%
	AVS (Address Verification Service)	38%	46%
	Geographic indicators/Maps	36%	24%
	Telephone number verification/Reverse lookup	36%	24%
	Social networking sites	31%	18%
Proprietary data	Customer order history	52%	33%
	Order velocity monitoring	45%	23%
	Positive lists/Whitelists	45%	34%
	Fraud scoring model: company-specific	45%	26%
	Negative lists/Blacklists	44%	39%
	Proxy detection	43%	26%
	Customer website behavior/Pattern analysis	35%	27%
Multi-merchant data	Multi-merchant purchase velocity/Identity morphing models	43%	21%
	Shared negative lists/Shared hotlists	38%	35%
Purchase device tracing	Device fingerprinting	41%	30%
	Geo-location: mobile device/tablet	37%	38%
	Geo-location: traditional laptop/desktop	36%	37%

Base 1147 (Question asked in North America and Europe only)
Prioritize balance (n=219), Do not prioritize balance (n=928)
Question: How effective are each of the following tools in detecting eCommerce payment fraud?

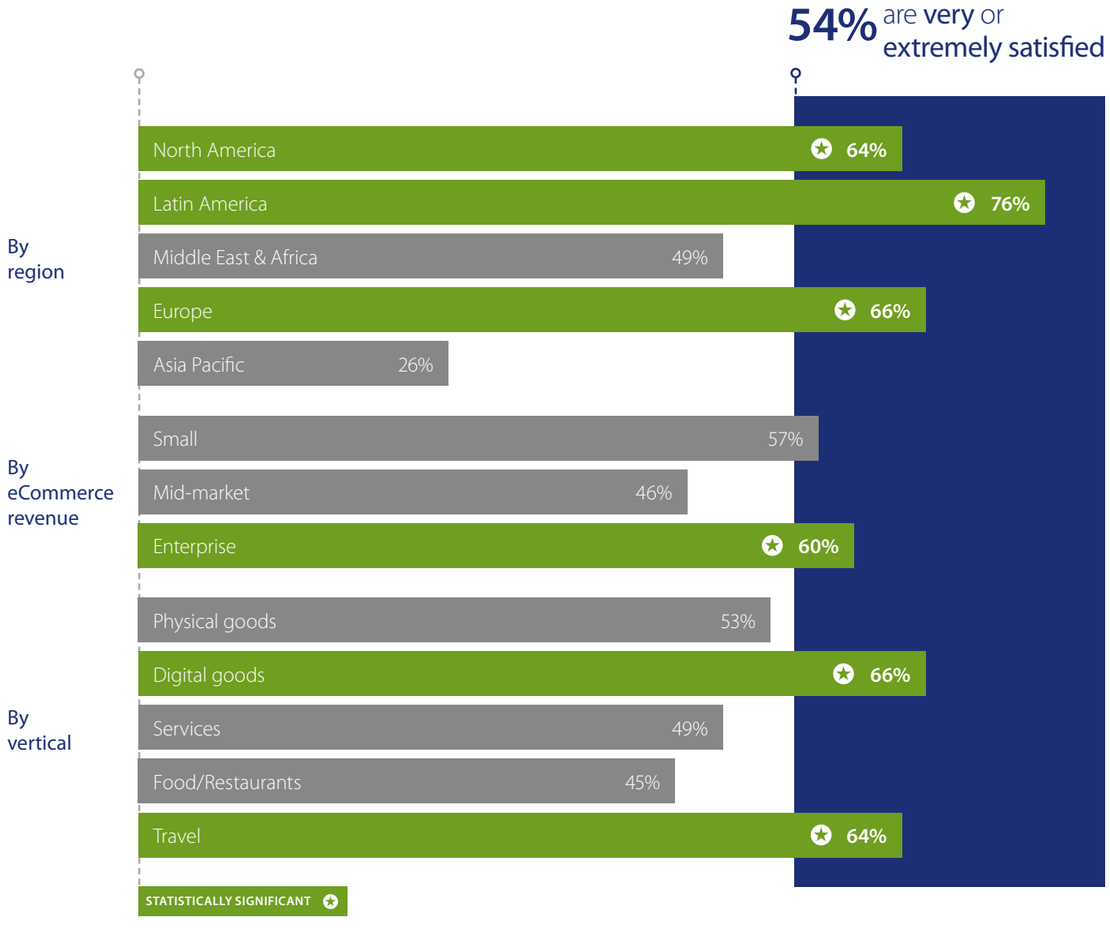
Dissatisfaction with tools is driving investment

The level of satisfaction with their arsenal of fraud prevention tools is one area in which there's no significant difference between the leaders and the rest.

Altogether, just over half (54%) of the respondents are very or extremely satisfied with the tools available to them (with only 12% in the 'extremely satisfied' group). This leaves a good deal of room for improvement in satisfaction levels.

Relative dissatisfaction with the available tools is driving widespread intent for all respondents to invest in tools they're not currently using. If these plans for investment are all acted on, then the five most-used tools today—CVN, customer order history, email verification, 3-D Secure and in-house negative lists—will remain the most-used (see *Figure 15*).

Figure 14. Satisfaction with fraud prevention tools



Base 1710 (Question not asked in Asia Pacific) **Question:** How satisfied are you with the fraud prevention tools that are available to you?
Answer options: Extremely satisfied, very satisfied, somewhat satisfied, not very satisfied, not at all satisfied

Enterprise interview respondents cited a key source of dissatisfaction as the lack of a single solution to meet their needs and they are having to integrate several best-in-class tools to create a best-fit solution. Some smaller organizations are very satisfied with outsourcing most of their fraud management to a trusted third party. Others believe that most tools are too expensive to invest in, often exceeding the fraud they are trying to mitigate.

> I think that the challenge is that there is not one tool that solves all problems.
>
> So, what you are constantly doing is you have fraud managers in organizations essentially developing their own Frankenstein version of a fraud tool, where they take two, three, or four different fraud solutions and kind of place them on top of each other to get the required result.
>
> **Role:** Fraud Decision Maker | **Vertical:** Retail | **Country:** USA

Figure 15. Fraud screening tool use: current and in a year's time

		Currently using	Plan to add in the next year
Validation services	CVN (Card Verification Number)	67%	20%
	Email verification	62%	26%
	Payer authentication (3-D Secure)	62%	25%
	AVS (Address Verification Service)	59%	25%
	Postal address validation services	53%	24%
	Two-factor phone authentication	45%	31%
	Credit history check	45%	30%
	Telephone number verification/Reverse lookup	45%	31%
	Search engine results	43%	30%
	Geographic indicators/Maps	43%	33%
	Social networking sites	40%	32%
	Biometric indicators	32%	36%
	Paid-for public record services	29%	34%
Proprietary data	Customer order history	67%	21%
	Negative lists/Blacklists (in-house)	60%	26%
	Positive lists/Whitelists	49%	28%
	Customer website behavior/Pattern analysis	46%	34%
	Fraud scoring model: company-specific	43%	34%
	Order velocity monitoring	39%	36%
	Proxy detection	38%	34%
Multi-merchant data	Multi-merchant purchase velocity/Identity morphing models	31%	38%
	Shared negative lists/Shared hotlists	44%	31%
Purchase device tracing	Geo-location: mobile device/tablet	51%	27%
	Geo-location: traditional laptop/desktop	47%	30%
	Device fingerprinting	30%	39%

MOST USED

LEAST USED

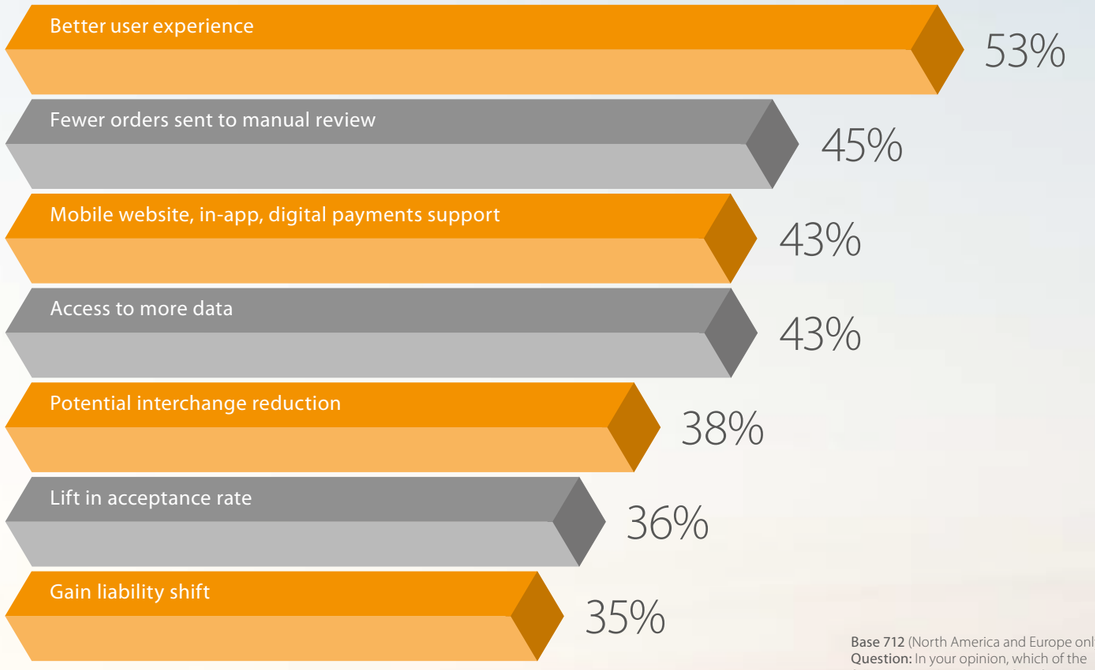
Base 1147 (Question asked in North America and Europe only)
Question: Next is a series of fraud detection tools. For each, please indicate whether your organization…
Answer options: Currently uses this tool, plans to add it in the next year, or neither

The new face of 3-D Secure

Despite historic concerns over a poor customer experience leading to cart abandonment, 3-D Secure (3DS) is one of the most-used tools in the fraud management toolkit.

This popularity probably reflects the fact that 3DS has increasingly become risk-based. Instead of challenging every transaction, issuers only challenge those shown to be a fraud risk through transaction risk analysis. In fact, the most frequently selected 3DS benefit is now 'better user experience' (with no difference between leaders and others).

Figure 16. Benefits of 3-D Secure
(% of 3-D Secure users selecting top benefits)



Base 712 (North America and Europe only)
Question: In your opinion, which of the following are the top benefits of using Payer Authentication (3-D Secure)?

The introduction of 3DS 2.0 in 2018 has delivered even more benefits in the form of:

- Smoother, more consistent user experiences across shopping and payment channels, especially for mobile browsers, apps and wallets
- Greater data exchange between merchants and issuers, enhancing risk-based transaction analysis and authentication

PSD2: Stronger authentication, smoother payments

In Europe, the Revised Payment Services Directive (PSD2) came into force in January 2018, except for requirements relating to strong customer authentication (SCA). When these take effect from 14 September 2019, transactions over €30 will require SCA to be applied.[6]

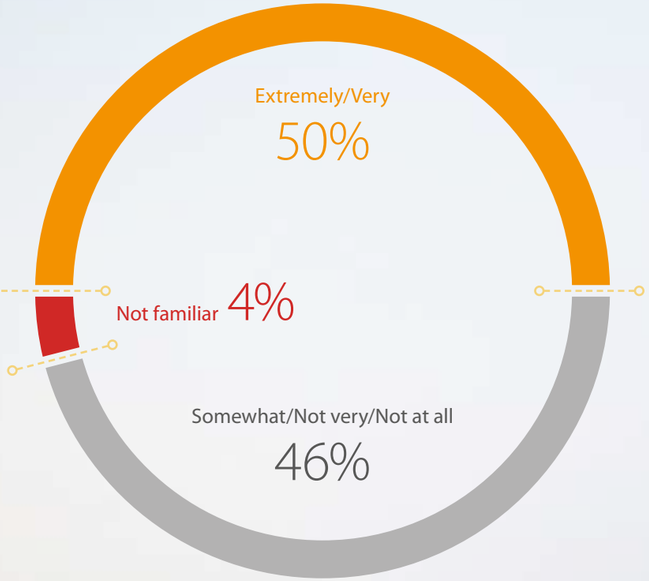
PSD2 SCA applies to payment transactions where both the issuer and acquirer are located in the European Economic Area (EEA).

This will require the buyer to present two or more of the following:

- Something they know *(e.g. one-time password, PIN)*
- Something they have *(e.g. token generator, mobile device, plastic card)*
- Something they are *(e.g. thumbprint, voice match)*

Only 50% of the European respondents feel prepared for PSD2 SCA.

Figure 17. Preparedness for PSD2 among European respondents



Base 817 (Europe results only)
Question: How prepared would you say your organization is for PSD2?

To improve your readiness:

- Review your authentication strategy, making sure it can support the requirement for strong customer authentication by 14 September 2019
- Understand how exemptions such as whitelisting and transaction risk analysis can be applied to help optimize the customer experience once SCA takes effect
- Maintain a robust fraud screening strategy, as the ability to apply exemptions will be influenced by fraud rates

This connection between SCA exemptions and fraud rate creates a new, more direct link between the customer experience and fraud management, making the balancing act even more important in future.

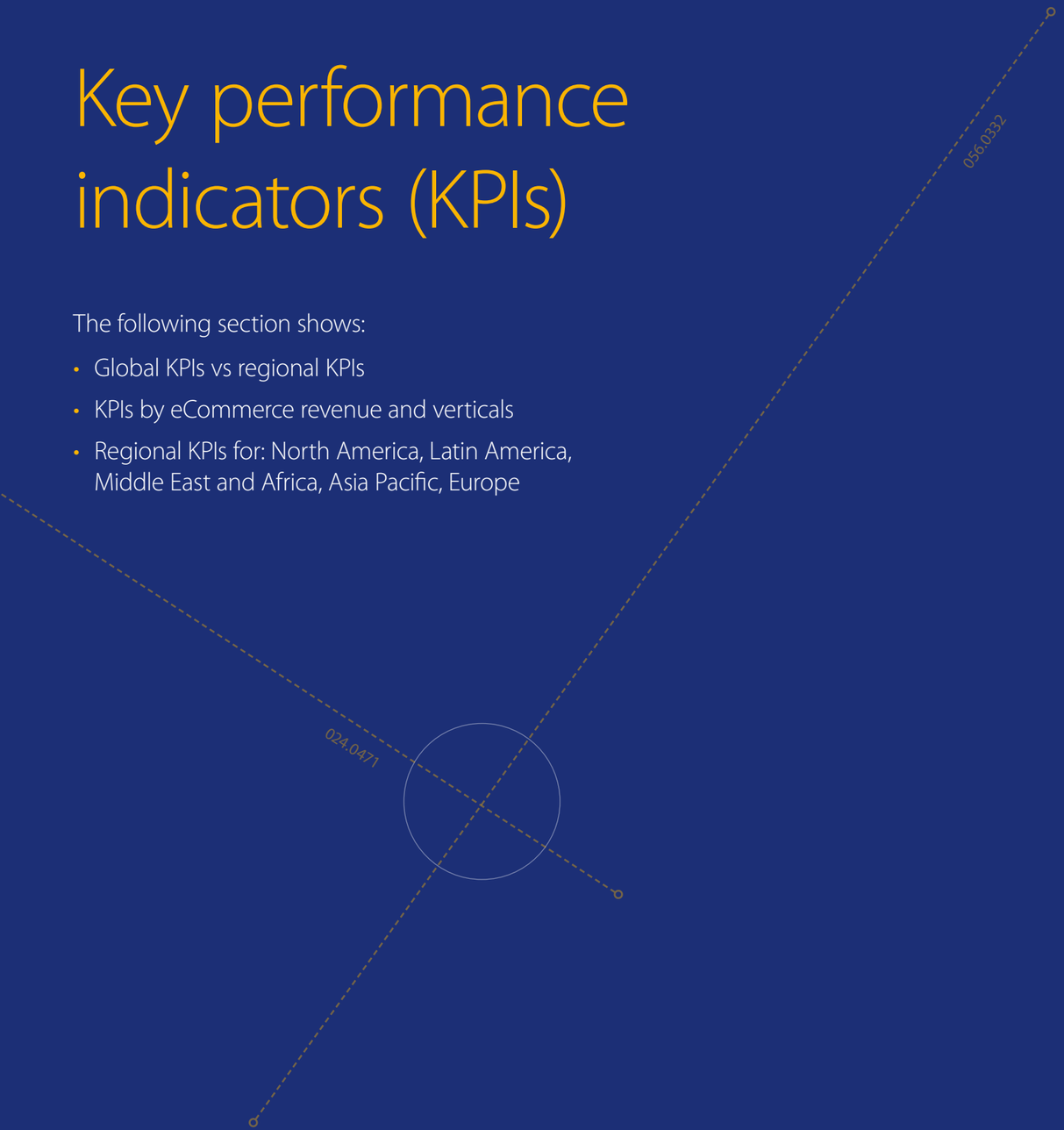
For more information on PSD2 and SCA, visit www.cybersource.co.uk/psd2[7]

[6] Except for transactions not in scope of the Directive or that have a valid exemption applied [7] This information is not intended to be legal advice nor a substitute for legal counsel

Key performance indicators (KPIs)

The following section shows:

- Global KPIs vs regional KPIs
- KPIs by eCommerce revenue and verticals
- Regional KPIs for: North America, Latin America, Middle East and Africa, Asia Pacific, Europe



KPI global overview

	Region							
	Global	North America	Latin America	Middle East & Africa	Asia Pacific	Europe (total)	Northern Europe	Southern Europe
% of annual eCommerce revenue lost due to payment fraud on domestic orders	1.6	1.5	1.3	1.8	1.5	1.9	1.6	2
% of domestic eCommerce orders rejected due to suspicion of fraud	2.5	3	2.8	3	2	3	2.7	4
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.3	0.7	0.6	0.7	0.1	0.7	0.6	0.7
% of eCommerce orders manually screened for fraud	25	16	20	30	30	20	20	25
% of eCommerce orders declined after manual review	3	10	20	15	1	10	11	8

	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

The results in the 2019 Global eCommerce Fraud Management Report are not recommended for year-on-year comparisons with previous regional CyberSource fraud reports. For this report, the global survey was based on a different sample and methodology, which was developed to give a more holistic picture of fraud today at a global level.

Note: Medians are shown for all KPIs

KPI overview by region

If you would like more detail on specific KPIs by country or how your business compares, please contact your Account Manager or contact CyberSource at www.cybersource.com/locations

	Region	eCommerce Revenue			Verticals				
	North America	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	1.5	2	1.2	1.3	2.5	3	1.9	1
% of domestic eCommerce orders rejected due to suspicion of fraud	3	2.9	4	2.7	3	4.5	4.6	4.5	2.5
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.7	0.8	0.7	0.6	0.6	0.6	1	0.9	0.6
% of eCommerce orders manually screened for fraud	16	25	20	10	17.5	21	15	18	12.5
% of eCommerce orders declined after manual review	10	5	8	15	9.5	15	5	4.5	22.5

	Region	eCommerce Revenue			Verticals				
	Latin America	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	1.3	1.3	1.5	1.2	1.4	1.2	5	3.1	1.3
% of domestic eCommerce orders rejected due to suspicion of fraud	2.8	2.6	2.9	3	2.8	3	5	10	2.5
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.6	0.6	0.6	0.6	0.5	0.6	4	5	0.6
% of eCommerce orders manually screened for fraud	20	25	26	12	15	12	33	12.5	25
% of eCommerce orders declined after manual review	20	20	28.5	15	20	10	11	20	32

Note: Medians are shown for all KPIs

	Region	eCommerce Revenue			Verticals				
	Middle East & Africa	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	1.8	2	1.5	3	1.7	5	3.5	8.5	4
% of domestic eCommerce orders rejected due to suspicion of fraud	3	2.9	2.8	4	2.8	10	3.7	5.5	2.3
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.7	0.6	0.8	0	0.7	3	0.3	6	0.8
% of eCommerce orders manually screened for fraud	30	36	23	23.5	30	37.5	42.5	10	32.5
% of eCommerce orders declined after manual review	15	17.5	20	10	20	20	15	8	12.5

	Region	eCommerce Revenue			Verticals				
	Asia Pacific	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	1.5	2	2	1	1.1	3.1	1
% of domestic eCommerce orders rejected due to suspicion of fraud	2	2.2	2	2	2.4	2	2	3	2
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.1	0.1	0.1	0.2	0.1	0.2	0.2	0.05	0.2
% of eCommerce orders manually screened for fraud	30	30	30	25	25	40	30	14	32.5
% of eCommerce orders declined after manual review	1	1	1	1	1.5	1	1	3	1

	Region	eCommerce Revenue			Verticals				
	Europe (total)	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	1.9	1.6	2	2	1.9	2.2	2	1.4	1.5
% of domestic eCommerce orders rejected due to suspicion of fraud	3	3	3.2	3	3	4	3	2.9	2.8
Fraud coded chargeback rate, as a % of annual eCommerce revenue	0.7	0.6	0.6	0.8	0.7	0.9	0.7	0.6	0.7
% of eCommerce orders manually screened for fraud	20	25	24	15	25	17	25	20	15
% of eCommerce orders declined after manual review	10	7	10	10	10	8	8	9	22.5

Note: Medians are shown for all KPIs

About this report

For a number of years, CyberSource has conducted regionally focused eCommerce fraud management surveys. This year, the survey has been taken to the next level in scale, capturing a robust and representative global sample.

Using the expertise of market research firm GfK, we have captured the views of nearly 2,800 fraud management specialists from small, mid-market and enterprise-level organizations. They represent 34 countries across North America, Latin America, Europe, the Middle East, Africa and Asia Pacific.[8] Along with securing representation across **five verticals**.

Respondent roles

Quantitative;
2,769 respondents comprising those who:

- Make or influence eCommerce fraud management decisions: 49%
- Are involved in eCommerce fraud management: 51%

Qualitative;
49 respondents across 15 markets participated in a post quantitative survey

[8] The survey was primarily conducted in April–June 2018. In South East Asia and Australia, the survey was conducted in October and November 2017

Figure 18. Geographical distribution of revenue representation

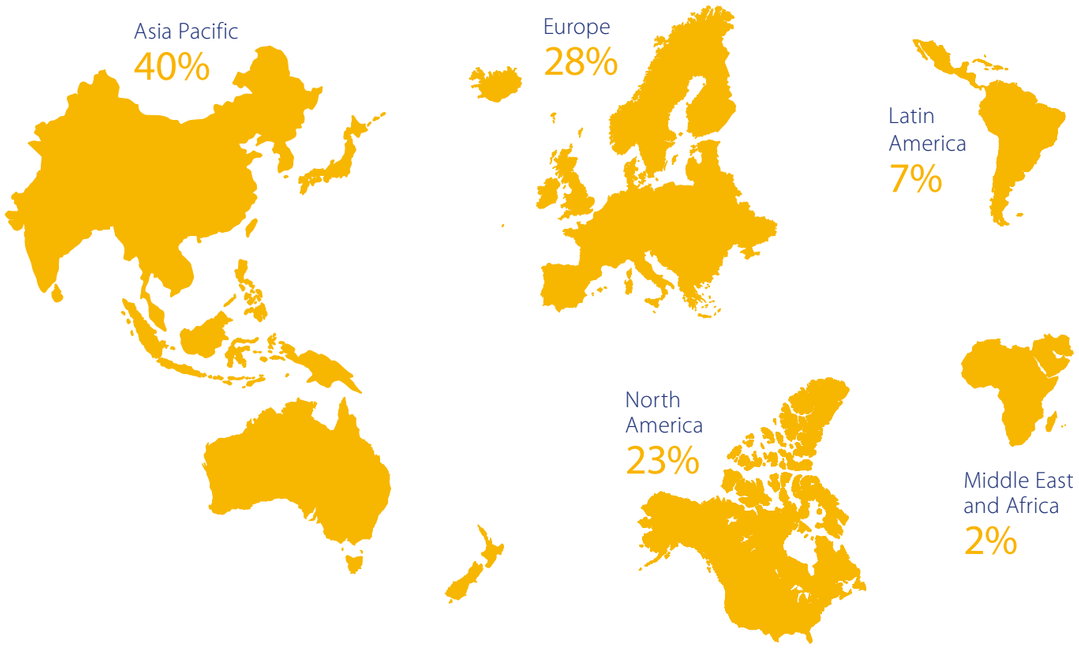


Figure 19.
Size of business by annual eCommerce revenue

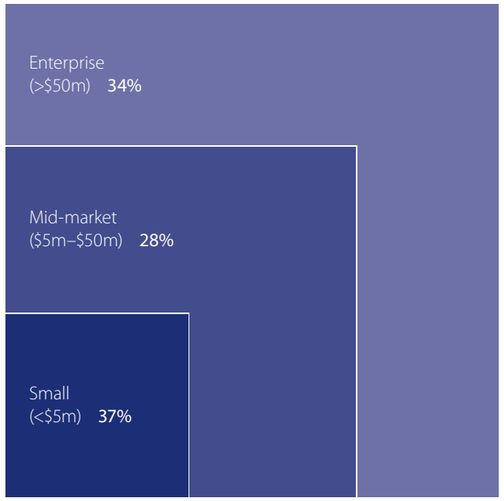
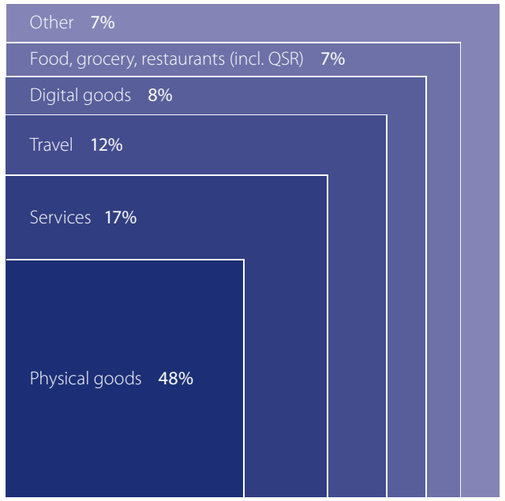


Figure 20.
Market sectors



How CyberSource can help

The digital economy continues to evolve, requiring many businesses to reassess their fraud management processes. As customers engage with you across multiple channels, using a variety of devices, you should have a balanced approach to fraud.

CyberSource can help you implement that approach, providing a complete range of fraud management solutions that help enable you to identify fraud quicker, more accurately, and with less manual intervention. We offer an end-to-end solution to support PSD2 SCA exemptions, with a variety of capabilities designed to keep customers data safe, increase acceptance and importantly, maintain a low fraud rate to potentially benefit from PSD2 SCA exemptions.

CyberSource Enterprise Fraud Management

CyberSource Enterprise Fraud Management is a multilayered fraud management solution that spans account monitoring, transaction fraud detection, rules tuning, and payer authentication. Accept more good orders, streamline operations, and gain agility. Fine-tune screening models and strategies—regardless of whether based on relationships—or stretch across multiple channels, various devices, or different levels of service.

Decision Manager

Automate and streamline your fraud operations with CyberSource Decision Manager—the only fraud management solution that gains machine learning insights from more than 68 billion transactions processed worldwide by Visa and CyberSource annually. Take advantage of a flexible rules engine to customize rules and models to your specific business across all sales channels, including web, mobile, call center, and kiosk channels. The combination of static and dynamic machine learning models are continually updated via real-time feedback loops, providing highly accurate scoring.

Rules Suggestion Engine

Unique in the fraud management arena, CyberSource Rules Suggestion Engine applies machine learning to the generation of rules, based on your own transaction history. Rules Suggestion Engine creates rules that are not humanly possible—taking only minutes to evaluate millions of combinations that could help reduce false positives, lower manual review rates and catch more fraud up front. Combining Rules Suggestion Engine with Decision Manager Replay gives you a powerful duo to keep up with ever changing fraudster tactics.

Decision Manager Replay

CyberSource Decision Manager Replay lets you confidently quantify the impact of your rule changes in real time, before activating them in your live production environment.
An industry first, Decision Manager Replay lets you quickly compare various "what-if" rules profiles against your own historical data, rather than waiting months to understand the impact of fraud changes. Decision Manager Replay produces real-time insights into likely changes to the transaction disposition and fraud rates, within minutes, before you push rules changes live.

Consulting Services

Managed Risk Services

Complement your in-house skills and resources with the global team of CyberSource fraud management experts. Managed risk analysts who serve clients on six continents can help you optimize CyberSource Decision Manager results and scale operations. This global knowledge network helps identify new fraud trends before they affect your business. Risk screeners are also available 24/7 around the world to augment or help manage all of your manual review during off hours and peak seasons. Count on CyberSource to be your trusted partner as your business expands.

Add-on Services

Account Takeover Protection

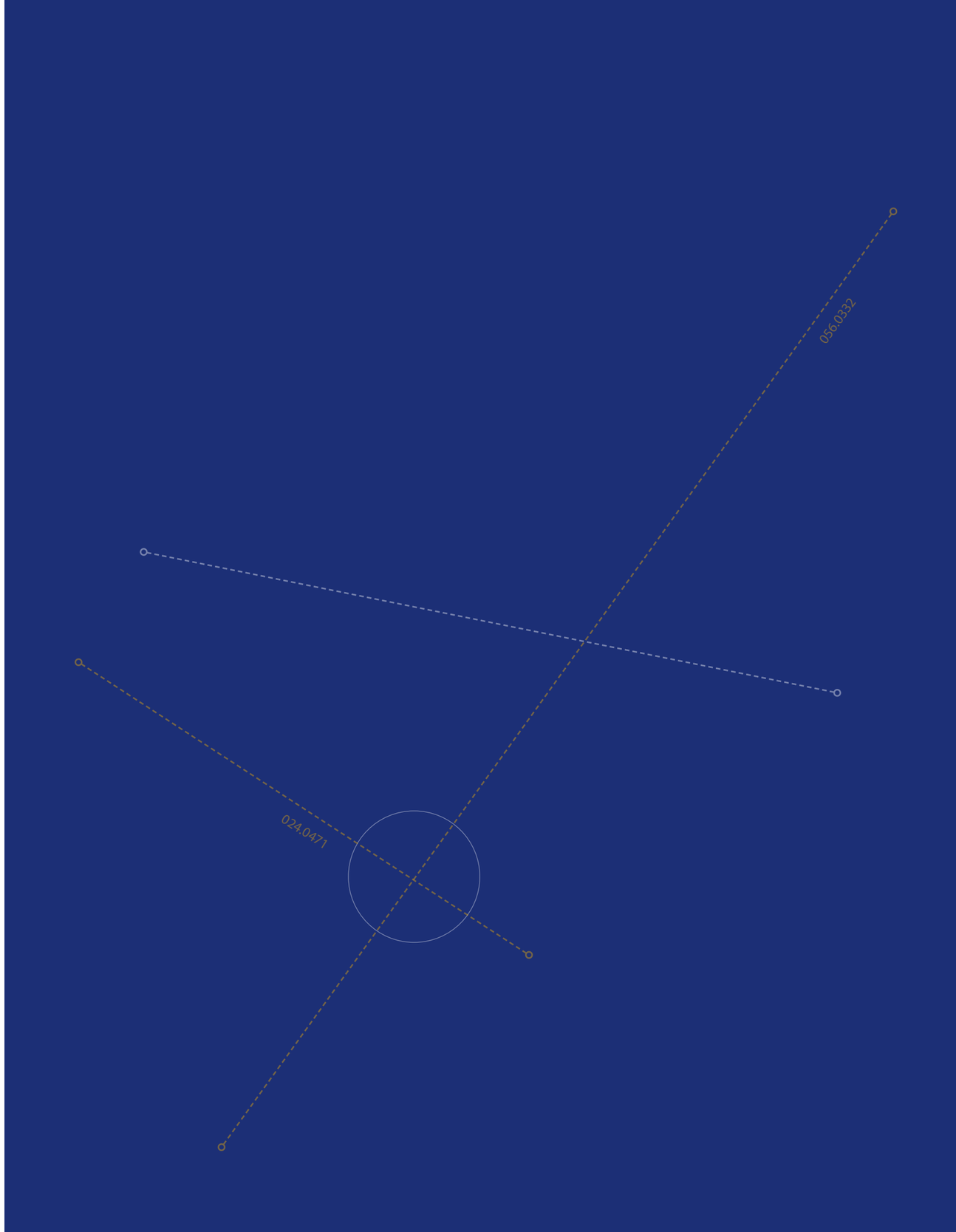
Account takeover fraud is an increasingly prevalent type of online threat that occurs when a fraudster exploits a victim's personal information to take control of an existing account or establish a new account. The fraudster then uses the account to carry out unauthorized transactions. CyberSource Account Takeover Protection defends customers and merchants from fraudulent uses of online accounts. It helps identify high-risk users at account creation and login, and monitors for suspicious account changes. With Account Takeover Protection, you can help keep your customer accounts safe and protect against fraudulent card-on-file payments while streamlining access for authenticated customers.

Loyalty Fraud

Complement your in-house skills and resources with the global team of CyberSource fraud management experts. Managed risk analysts who serve clients on six continents can help you optimize CyberSource Decision Manager results and scale operations. This global knowledge network helps identify new fraud trends before they affect your business. Risk screeners are also available 24/7 around the world to augment or help manage all of your manual review during off hours and peak seasons. Count on CyberSource to be your trusted partner as your business expands.

Rules-Based Payer Authentication

CyberSource Rules-Based Payer Authentication provides you with control over your customer experience along with all the benefits of traditional 3-D Secure, including the liability shift and reduction of interchange fees. You decide at what risk level to request payer authentication protection so you can guard against fraud and deliver more seamless checkout experiences for your customers.



Limitation of liability

The information, recommendations or "best practices" contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for business, operational, marketing, financial, legal, technical, tax or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or "best practices" may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. CyberSource is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. CyberSource makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, CyberSource shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Contact us

For contact information please visit www.cybersource.com/locations

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

CyberSource®
A Visa Solution