FT LONGITUDE

On the right side of AI

Shaping the future of payment fraud prevention

SURVEY REPORT
JUNE 2025

CONTENTS

01

Introduction

Introduction

The rise of large language models (LLMs) and generative AI (Gen AI) is enabling organizations to bolster their defenses against an onslaught of payment fraud.

These tools give organizations the capability to sift through a mountain of transactions, identifying subtle patterns that could constitute warning signs, and anticipate fraudsters' future tactics.

But organizations need to maximize the benefits of these AI-powered systems. This means employing data and governance tactics to enhance their effectiveness. They must also find ways to share intelligence securely and responsibly between disparate systems and data sources to make sure they identify genuine threats rather than generate time-wasting false positives.

Globally, the financial impact of fraud was estimated at above $485 billion in 2024. As Gen AI makes it easier and more affordable for malicious actors to launch increasingly sophisticated, targeted and disguised attacks, this threat is projected to continue to rise.

This report draws on a survey of 300 senior fraud and risk-mitigation executives in the payment industry from mid-sized and large organizations worldwide, with annual revenues ranging from $50 million to over $100 billion. The research explores how the payment industry is using AI to protect businesses and customers from fraud and outlines how businesses can further enhance their defenses.

This report uses an inclusive definition of AI to capture the impact of various AI tools on payment fraud prevention, from newer forms of LLMs and Gen AI to more established neural networks and machine learning (ML) capabilities.

$485b+

Global impact of fraud: 2024

Characteristics of the leader group

To examine best practices, we identified a group of survey respondents who are using AI effectively to fight payment fraud. These 52 respondents (17% of the total sample) report that they are significantly reducing fraud rates and consistently generating a return on investment (ROI) from using AI in five or more of the following seven areas:

01 **Fraud case triage and investigation**

02 **Transaction pattern recognition**

03 **Real-time detection of suspicious transactions**

04 **Cross-channel fraud detection**

05 **Elimination of unnecessary manual reviews or processes**

06 **Behavioral biometrics**

07 **Predictive analytics**

Fast facts

85%

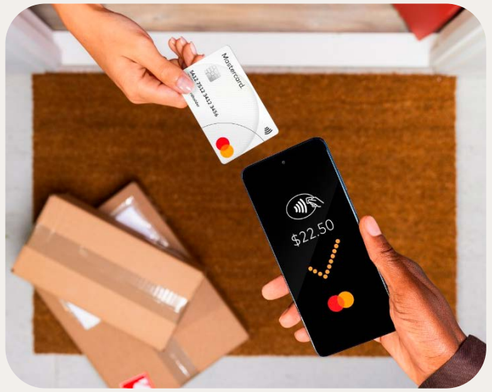
of respondents report seeing returns from using AI for fraud case triage and investigation, transaction pattern recognition and real-time detection of suspicious transactions.

90%

agree that failure to increase their use of AI in fraud prevention in the next three years will likely result in increased financial losses.

83%

say that AI has significantly accelerated fraud investigation and resolution.



$60m

On average, in the past 12 months, organizations in the payment industry have lost $60 million in annual revenue due to payment fraud.

83%

say that AI has significantly reduced false positives and customer churn rates in the past year.

64%

recognize the need to accelerate the rate at which they acquire new, credible data sources.

59%

note that external alliances focused on intelligence sharing are crucial to strengthening fraud prevention.

02

Current state of play and the road ahead

How AI is being used to combat payment fraud

Advancements in AI capabilities can be used to harm, as well as to protect.

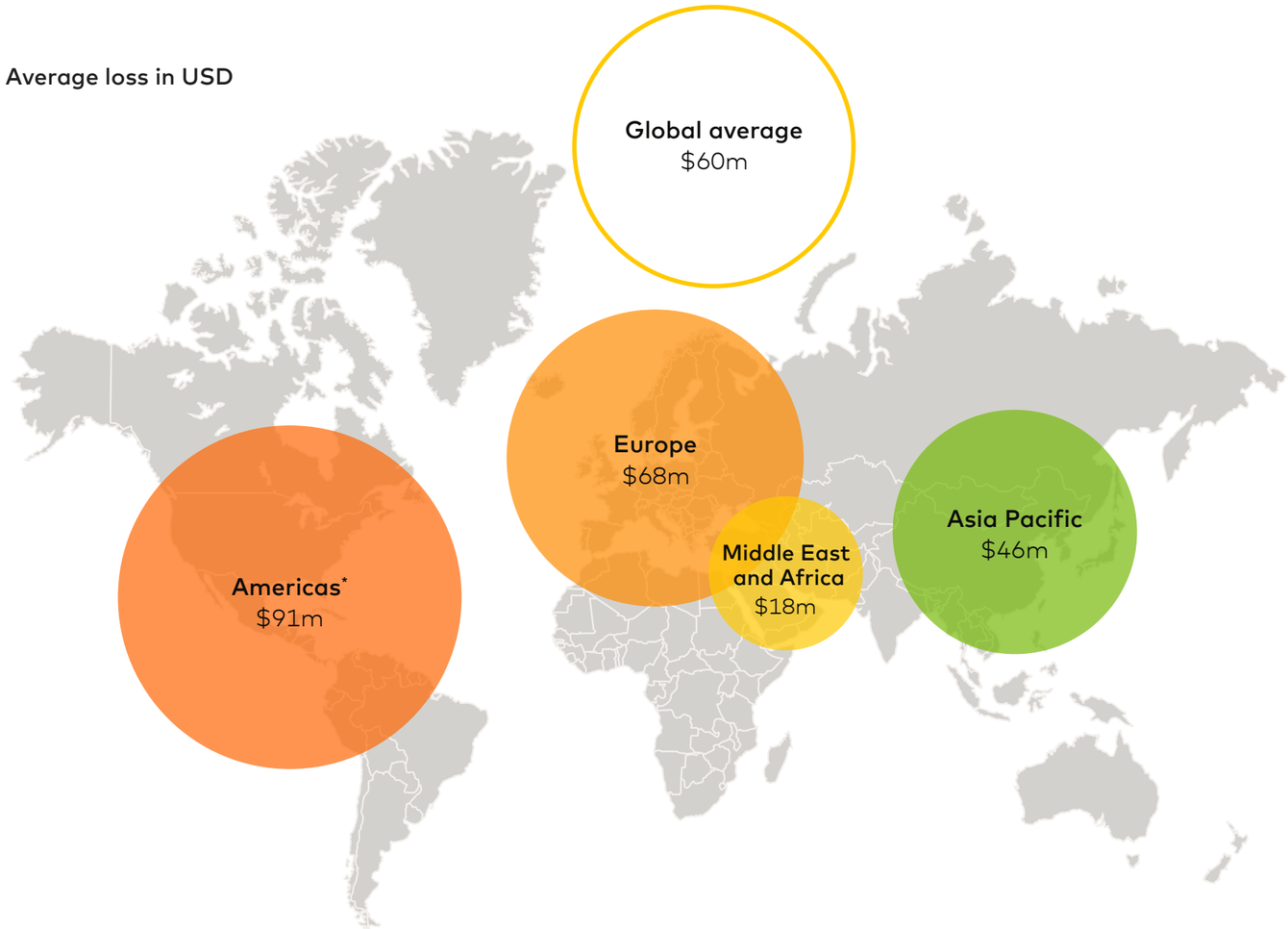
Malicious actors are using accessible and affordable AI-powered tools to automate fraud attempts and reach more victims. Gen AI can help improve the quality of written content or even create deepfake videos or voice clones, driving more effective social engineering techniques. These techniques exploit human interactions and emotions to manipulate targets into giving away sensitive information or compromising security.

"[Fraudsters] are reaching out to [victims] on a very personal level because they have a lot of data that's publicly available or at least can be extracted," says Kerry Thomas, Senior Vice President of Fraud and Decisioning Products at Mastercard. "AI not only allows [fraudsters] to do those kinds of nuanced behavioral things, but it also allows them to process through quickly. So, attacks happen all the time, remotely and at speed. It's a never-ending fight."

As banks have strengthened their cyberdefenses in recent years, fraudsters are increasingly targeting customers. The advent of real-time payments has narrowed the window of opportunity to block fraud attempts.

Figure 1

Regional average revenue losses in USD per organization due to payment fraud over the last 12 months



*Americas is comprised of Brazil, Canada, Mexico and United States

Stuart Skinner, Head of The Fraud Prevention Team at NatWest, has noticed payment fraudsters shifting away from tactics such as gaining unauthorized access to bank accounts. Instead, they are targeting customers. Authorized push payment fraud — when a bad actor tricks a victim into authorizing a payment to a fraudulent account — is increasingly widespread.

Skinner explains, "They will contact the customer and get codes, or they will get the customer to [make a payment or transfer] themselves, and that makes it difficult for us because we are looking for something unusual. And there is nothing unusual about this because it's the customer."

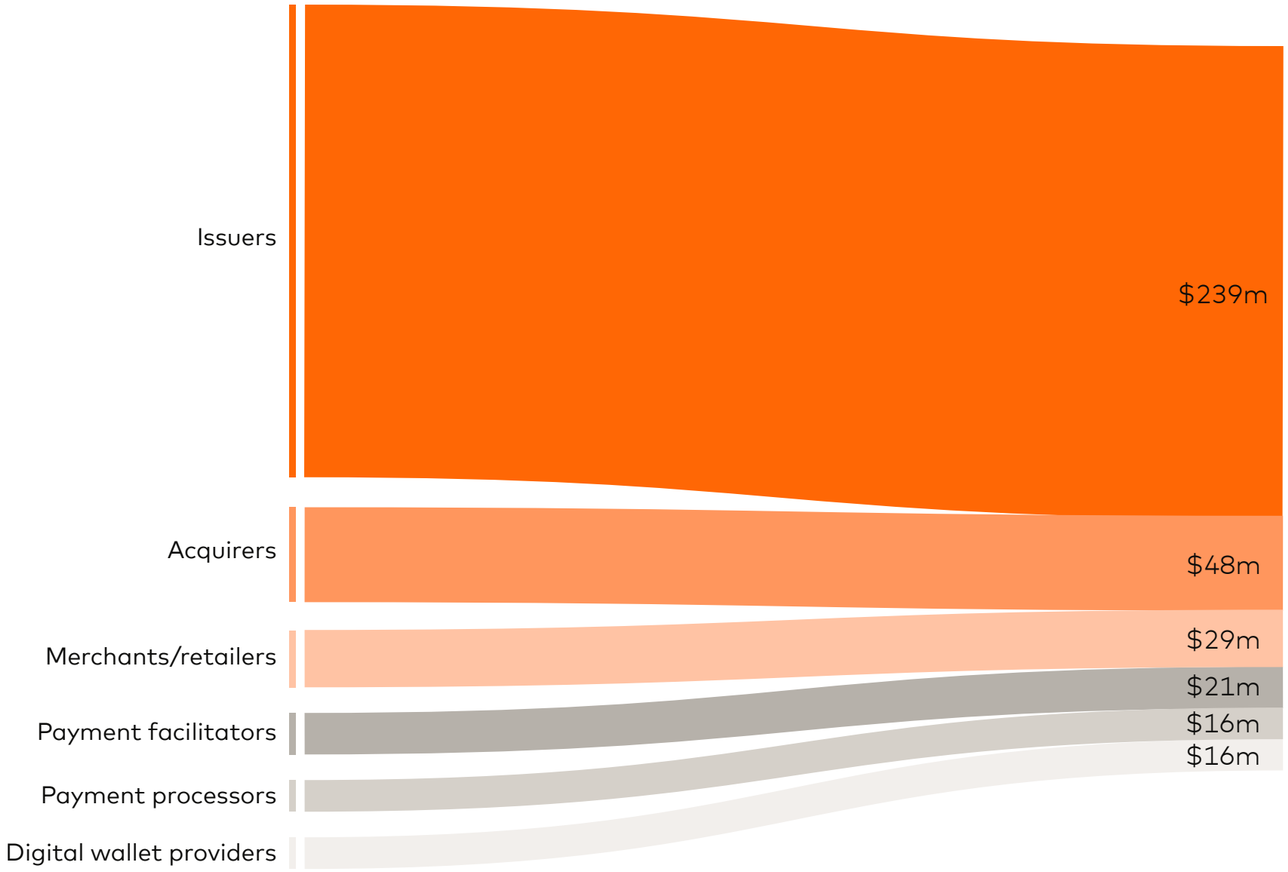
Also, if the victim initiates the transfer, they may have less legal protection and find it harder to be reimbursed. Bad actors are reaping the rewards. The organizations in the payment industry that we surveyed say that on average they have lost $60 million in revenue to payment fraud in the past year.

> ***Fraudsters are reaching out to victims on a very personal level because they have a lot of data that's publicly available or at least can be extracted.***

Kerry Thomas
Senior Vice President of Fraud and Decisioning Products, Mastercard

Figure 2

Flow diagram of losses in the payment journey per organization due to payment fraud over the last 12 months (by sector category)



This campaign's sample includes only mid-to large-sized companies in the payment industry. Specifically, those with annual revenues ranging from $50 million to $100 billion or more. For context, the average revenue within this sample is $2.8 billion.

But companies are using AI to fight back, and are stopping millions of dollars from falling into the hands of fraudsters. Some 42% of issuers and 26% of acquirers surveyed say they managed, with the help of AI, to save more than $5 million from fraud attempts in the last two years (Figure 3).

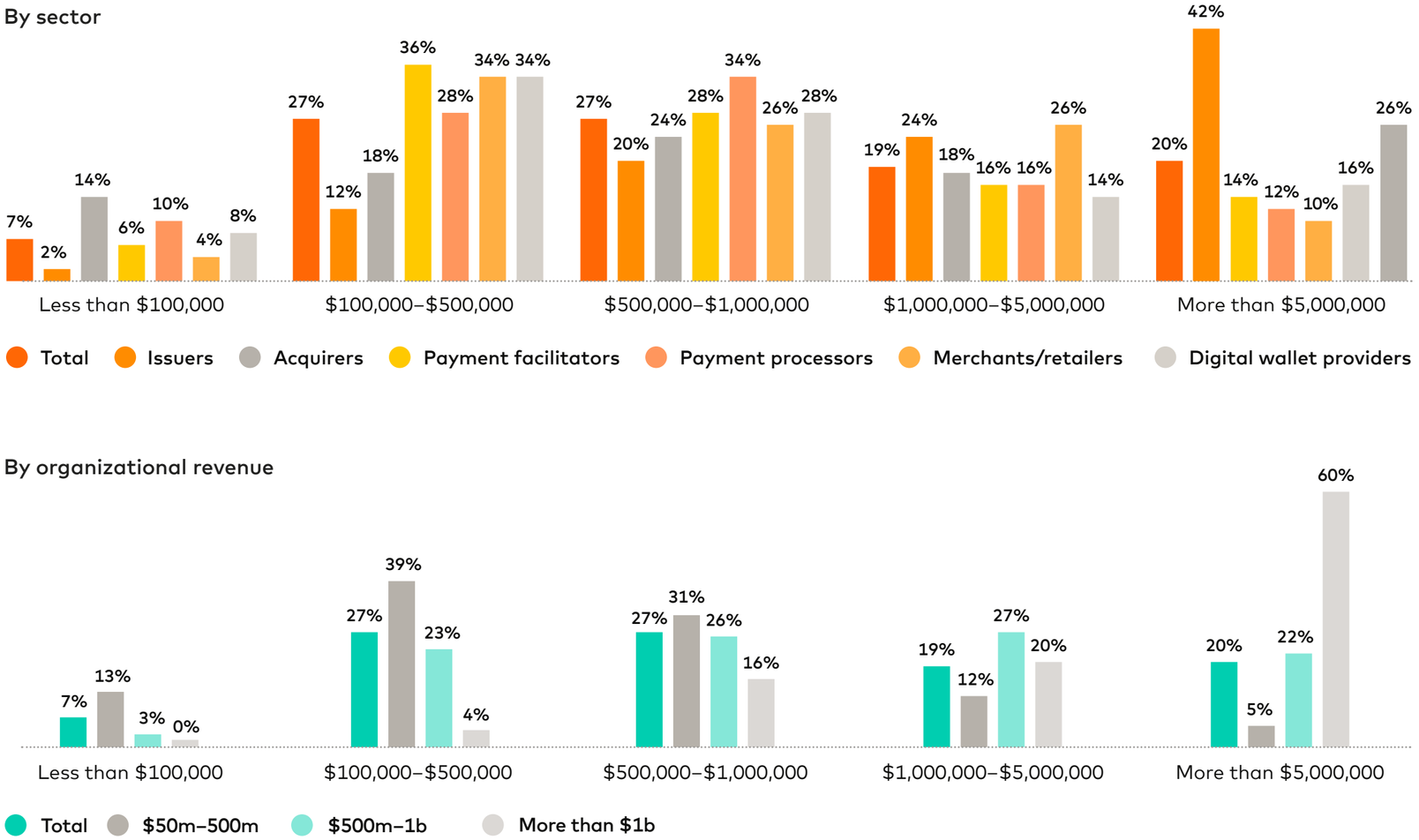
The rise of readily available, accessible and affordable Gen AI and LLM-based tools in the past couple of years has driven a dramatic uptake by businesses. As of early 2025, 78% of organizations were using AI[1] in at least one business function, a dramatic rise from 55% just two years prior. Although still in the relatively early days, these advanced tools are revolutionizing the payment industry.

"Financial services is undergoing a significant shift in fraud detection, moving from ML systems to AI-based methods," says Samantha Emery, Director of Payments Industry and Development at Lloyds Banking Group. "This transition has enhanced fraud prevention capabilities while reducing the number of false positives, helping many organizations further strengthen the ways they protect customers from harm."

[1] McKinsey, "The state of AI: How organizations are rewiring to capture value," 2025

Figure 3

Financial savings (USD) over the past two years from using AI in fraud prevention



Q: Approximately how much in USD has your organization saved over the past two years by using AI in fraud prevention?

Strengthening defenses

> *Using a combination of approaches — such as pattern identification and active monitoring of transactions using AI, two-factor authentication, end-to-end encryption and biometrics — makes it harder for fraud to be carried out.*

Samantha Emery
Director of Payments Industry and Development,
Lloyds Banking Group

AI-driven tools and systems are helping organizations to proactively and efficiently boost their cybersecurity defenses, enhance resilience and keep pace with emerging threats. "Historically, combating payment fraud would be a manual process of providing inputs on what transactions to allow and what to block," says Zachary Weinstock, Vice President of Finance at Lotto.com.

And while human intervention is still critical for performing checks and balances, Weinstock adds, "we've been able to rely on AI and ML at scale to increase the speed of fraud detection, anticipate threats and take some of the burden off humans." In some cases, Lotto's AI tools have led to a 50% reduction in fraud cases, with almost no negative impact on revenue.

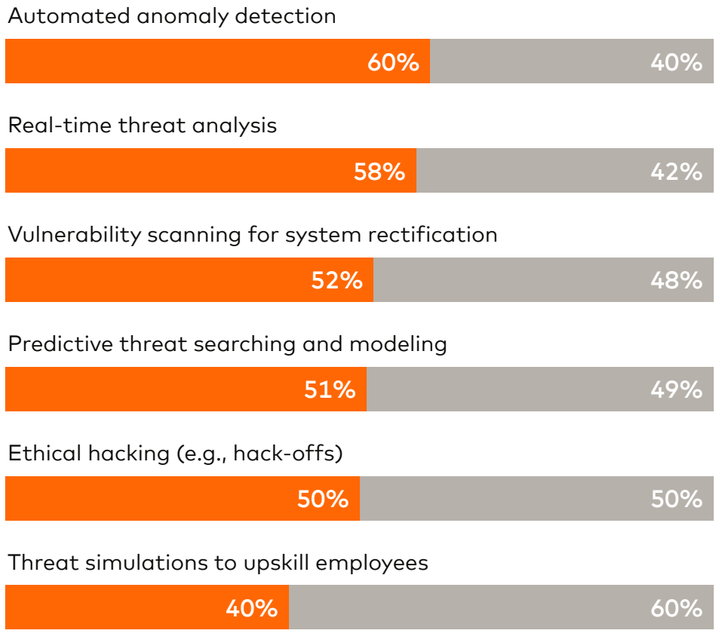
"Using a combination of approaches — such as pattern identification and active monitoring of transactions using AI, two-factor authentication, end-to-end encryption and biometrics — makes it harder for fraud to be carried out," adds Emery, outlining the "multi-layered approach" Lloyds Banking Group takes to fraud prevention.

Of our survey respondents, 60% use AI for automating anomaly detection, 58% for real-time threat analysis and 52% for vulnerability scanning. Predictive threat searching and modeling (51%), ethical hacking (50%) and simulating threats to upskill employees (40%) are not far behind (Figure 4).

The vast majority of our survey respondents see notable benefits from using AI for fraud detection. An impressive 83% say that AI has significantly reduced the time needed for fraud investigation and resolution, and the same percentage says that AI has helped them lower their false positives and customer churn rates (Figure 5).

Figure 4

The most popular AI tactics for strengthening cybersecurity defenses



Q: How is your company using AI to strengthen its cybersecurity defenses?

Organizations are already seeing a reduction in fraud rates and are generating ROI from various AI use cases. As many as 85% of respondents are seeing returns from implementing AI in fraud case triage and investigation. Some 53% cite a significant reduction, and of this group 18% say their activities are consistently generating ROI. Transaction pattern recognition — which can rapidly identify fraudulent activity hiding in layers of legitimate transactions — and real-time detection of suspicious transactions are seeing similarly impressive returns (Figure 6).

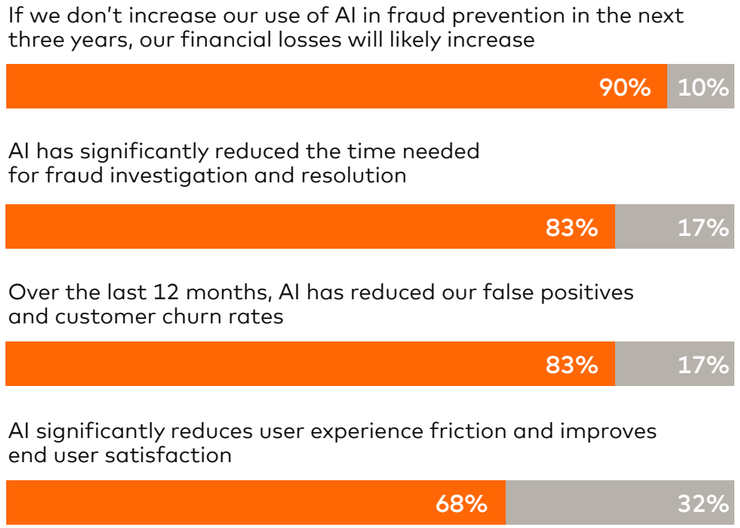
Our leader group is made up of respondents who say they are significantly reducing fraud rates or consistently generating ROI and minimizing fraud in the majority of these use cases (at least five out of seven).

83%

of survey respondents say that AI has significantly reduced the time needed for fraud investigation and resolution.

Figure 5

Most respondents consider AI to be a core pillar of their payment fraud prevention



Q: Do you agree or disagree with the following statements? (Agree summary)

Calculating the ROI of AI in fraud mitigation can be hard to quantify. The value of using AI for fraud mitigation comes in various forms, including improved operational efficiency, enhanced regulatory compliance and better customer satisfaction. Not all of these are easily quantified, however, especially when they are realized indirectly or over extended time frames. Crucially, measuring potential losses can be something of a guessing game.

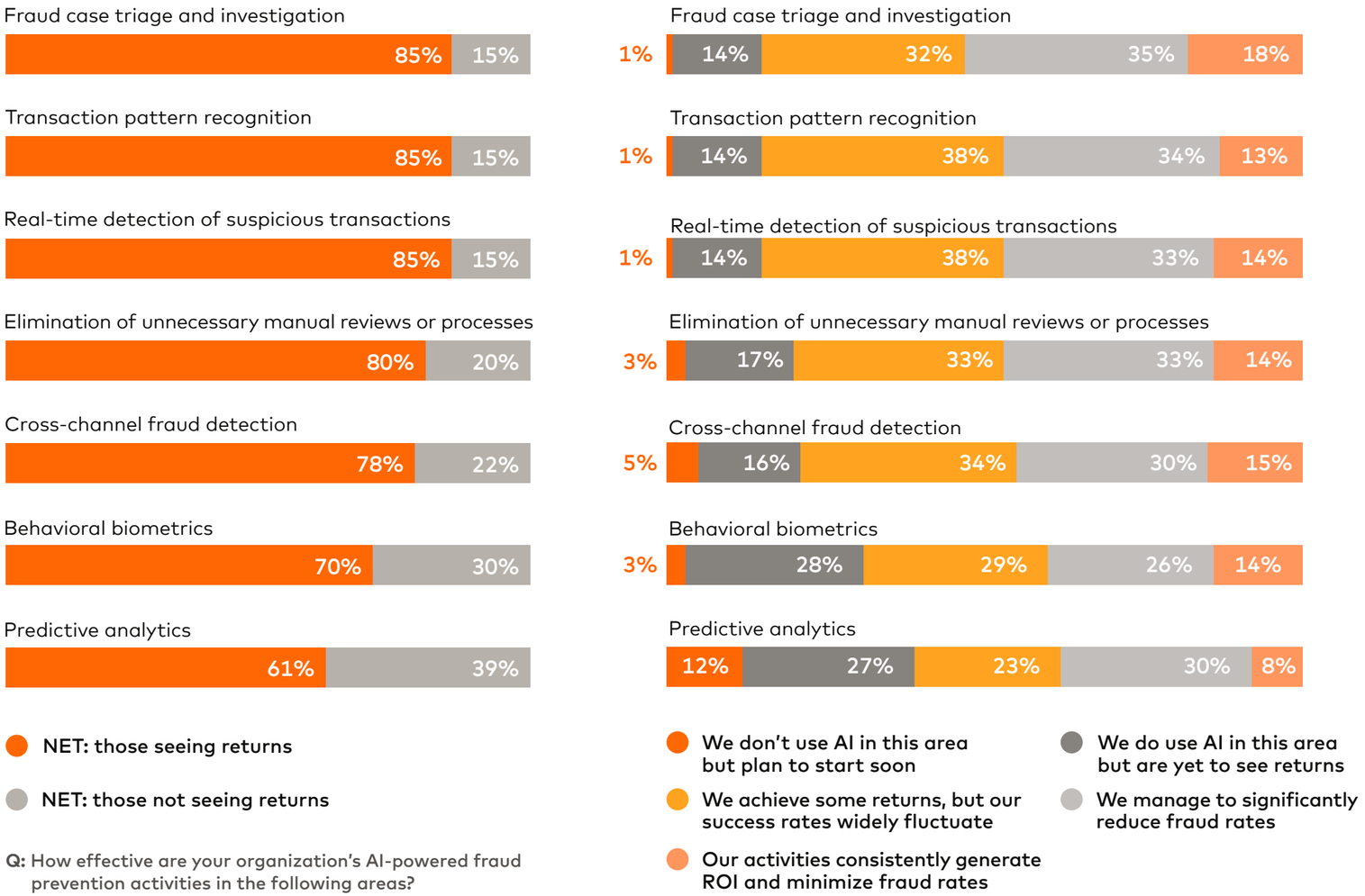
> *Organizations aiming to understand the ROI of AI in payment fraud prevention should focus on clear KPIs, baseline comparisons and continuous model evaluation.*

Laura Quevedo
Executive Vice President of Fraud and Decisioning Solutions, Mastercard

"Organizations aiming to understand the ROI of AI in payment fraud prevention should focus on clear KPIs, baseline comparisons and continuous model evaluation," says Laura Quevedo, Executive Vice President of Fraud and Decisioning Solutions at Mastercard. She adds that firms need to consider both the short- and long-term value generated. "By tracking fraud reduction rates, operational efficiency and customer impact, businesses can quantify the benefits of AI," she says.

Figure 6

Most respondents see returns from use cases that harness AI to combat payment fraud



Q: How effective are your organization's AI-powered fraud prevention activities in the following areas?

With AI, the rewards start to stack up

Our research indicates that there is a positive correlation between the length of time leveraging AI and success rates. For instance, those who have used AI for more than five years say that they have saved $4.3 million in lost revenue, nearly double the average savings ($2.2 million).

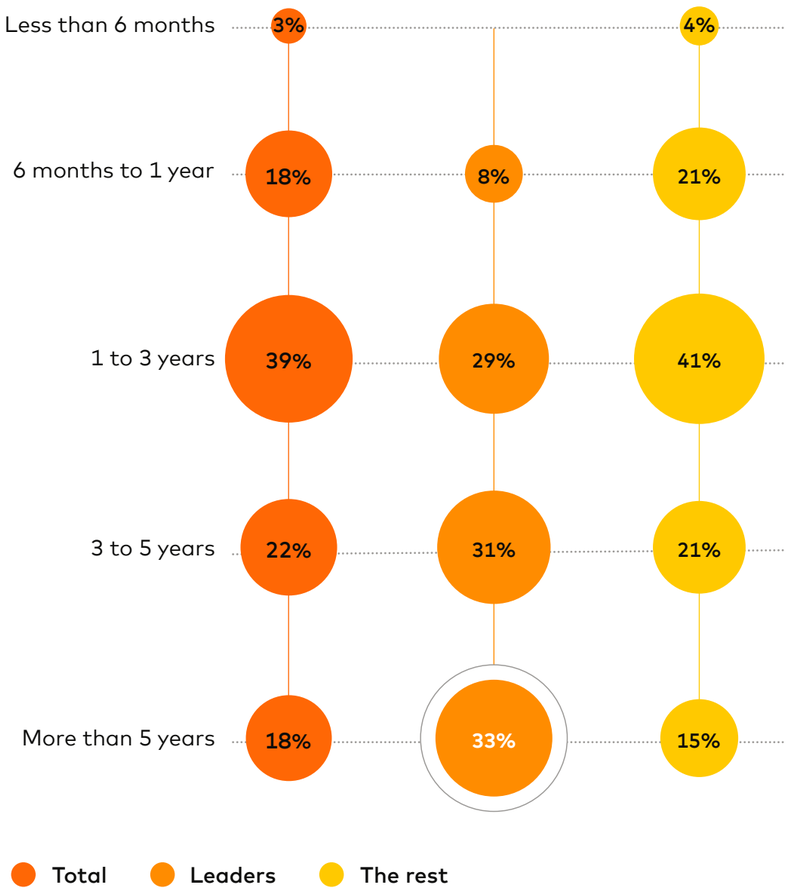
Overall, most (79%) of those surveyed have been using AI to combat fraud for at least one year, while 18% have been doing so for at least five years. Our leader group has been using AI longer, on average, than the rest, with 33% using AI for more than five years, which is 18 percentage points above non-leaders (Figure 7).

79%

of those surveyed have been using AI to combat fraud for at least one year.

Figure 7

Organizations that adopted AI for fraud prevention earlier are having the most success



Q: How long have you been using AI as part of your fraud prevention approach?

Keeping pace with growing threats

Given these cumulative benefits, there is an unsurprising keenness to expand AI use. Nearly all respondents (90%) agree that failure to increase their use of AI for fraud prevention in the next three years will result in increased financial losses (Figure 5).

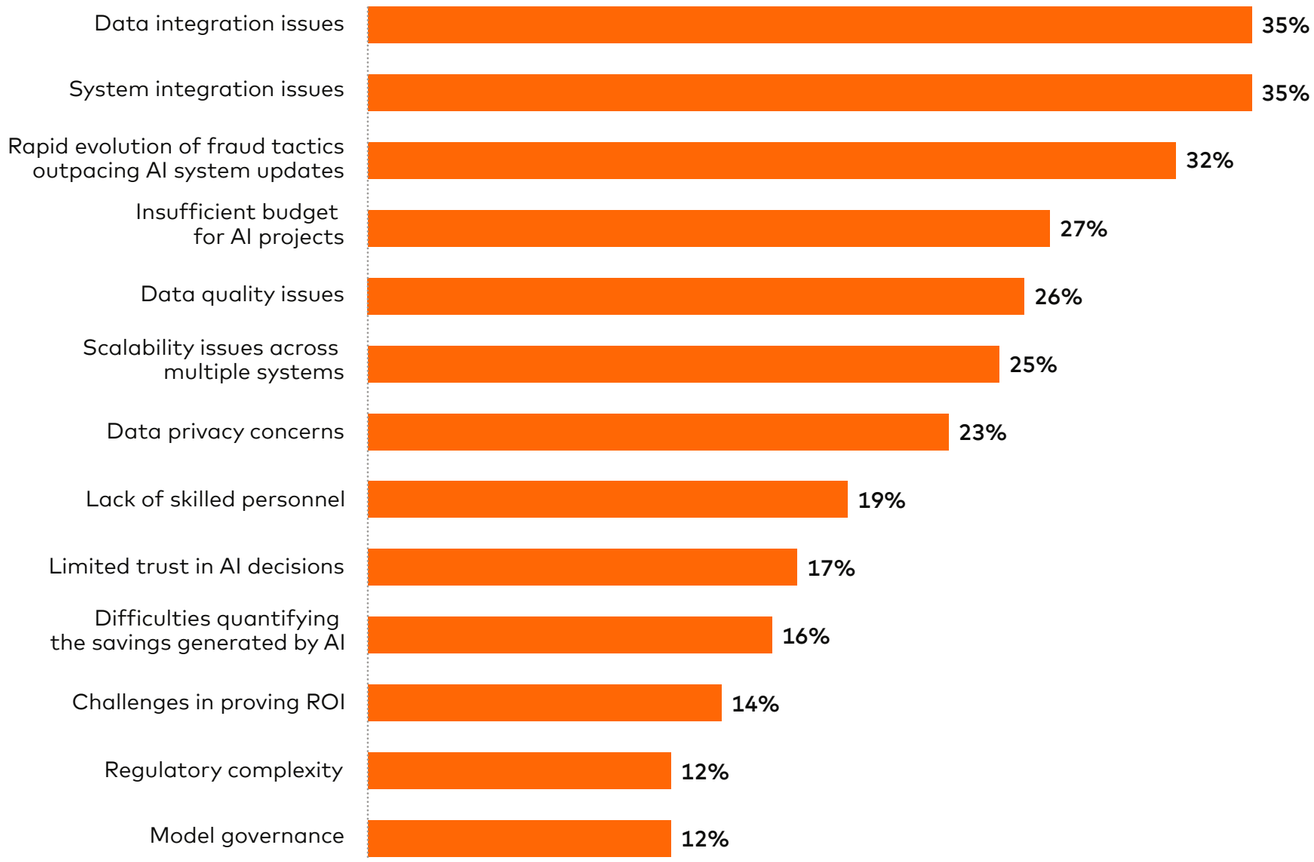
But keeping AI technology up to date with the rapid evolution of fraud tactics is a top three challenge for businesses (Figure 8). Our leaders say this is the toughest obstacle they face in successfully tackling payment fraud.

90%

of respondents agree that failure to increase their use of AI for fraud prevention in the next three years will result in increased losses.

Figure 8

Integration issues are the main obstacle to AI projects combating payment fraud



Q: Which of the following are the main obstacles in implementing AI projects to combat fraud?

Looking ahead, the survey respondents identify synthetic identity fraud as the fastest-growing threat in the next 12 months. This is an advanced form of identity theft where fraudsters use a mix of real and fake information to create a fictitious identity. This identity can then be used to open bank accounts, apply for loans or commit other types of financial fraud. This threat is closely followed by impersonation schemes (60%) and cross-border schemes (54%), where fraudsters illegally acquire funds during transactions between parties in different countries. They often use the complexities of global payment systems and regulatory differences to cloak themselves and evade detection (Figure 9).

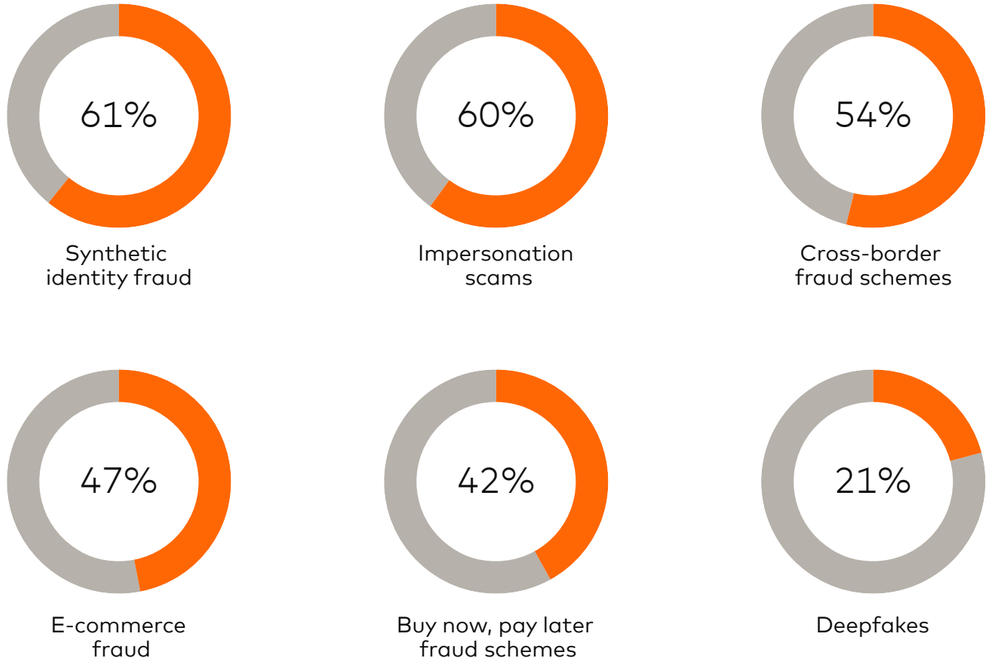
> *"Fraud and fraud patterns evolve rapidly, and the data leveraged to train models must keep pace.*

Brian McGuigan
Senior Vice President of AI Fraud Solutions, Mastercard

"Proactive and defensive AI integration will become more critical than ever for banks and other financial institutions that want to stay ahead," says Brian McGuigan, Senior Vice President of AI Fraud Solutions at Mastercard. "Fraud and fraud patterns evolve rapidly, and the data leveraged to train models must keep pace." Fresh data inputs and sharp governance strategies will be essential to keeping up with the evolving threat landscape. McGuigan adds, "Accessing new, credible data allows AI models to quickly adapt and identify emerging trends quicker and more precisely, enabling enterprises to gain a competitive edge."

Figure 9

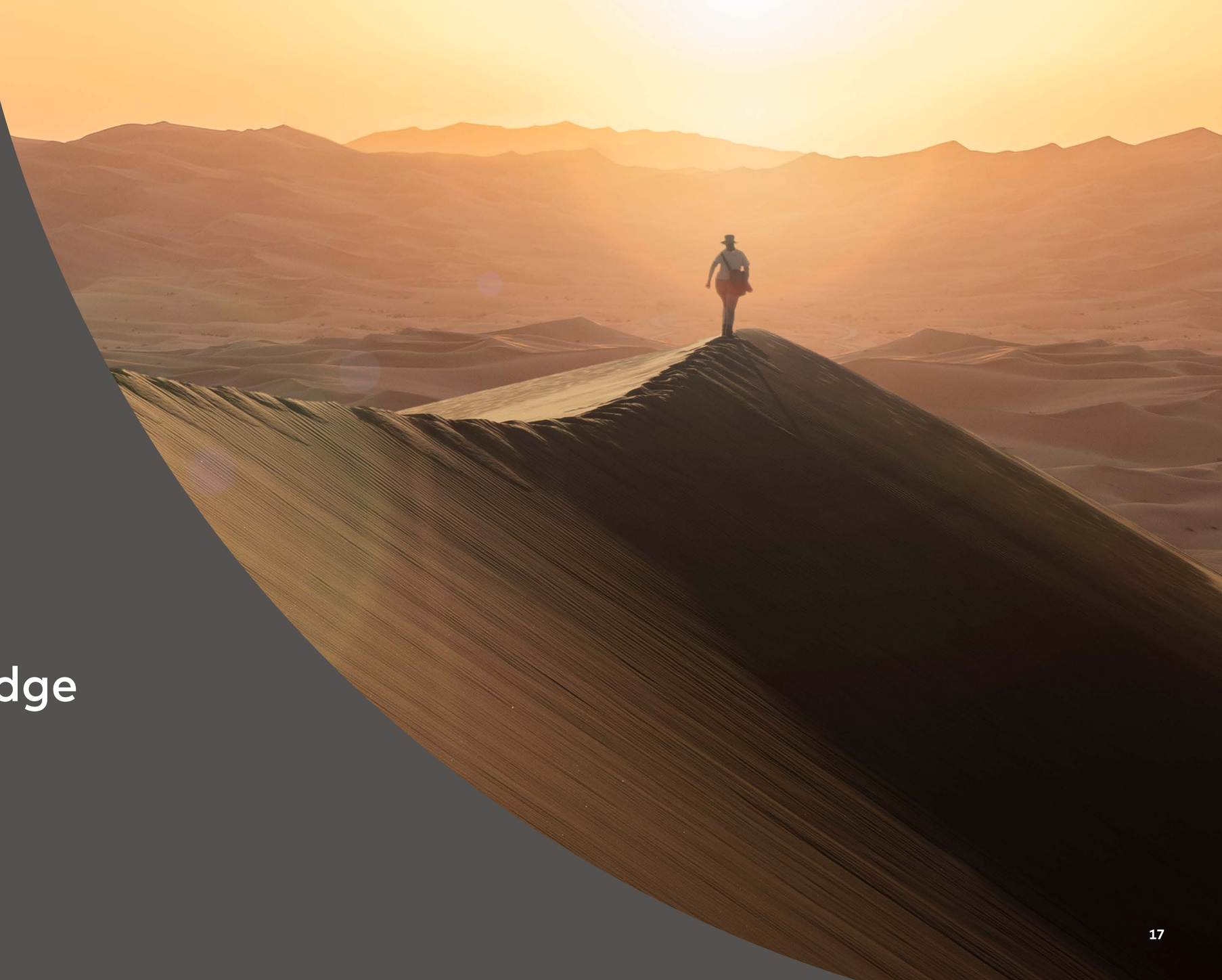
Most respondents expect synthetic identity fraud and impersonation fraud to be the fastest-growing threats over the next 12 months



Q: Which of the following, if any, do you foresee becoming an increasing threat over the next 12 months?

03

Data offers a competitive edge



Connecting the dots to reveal fraud risks

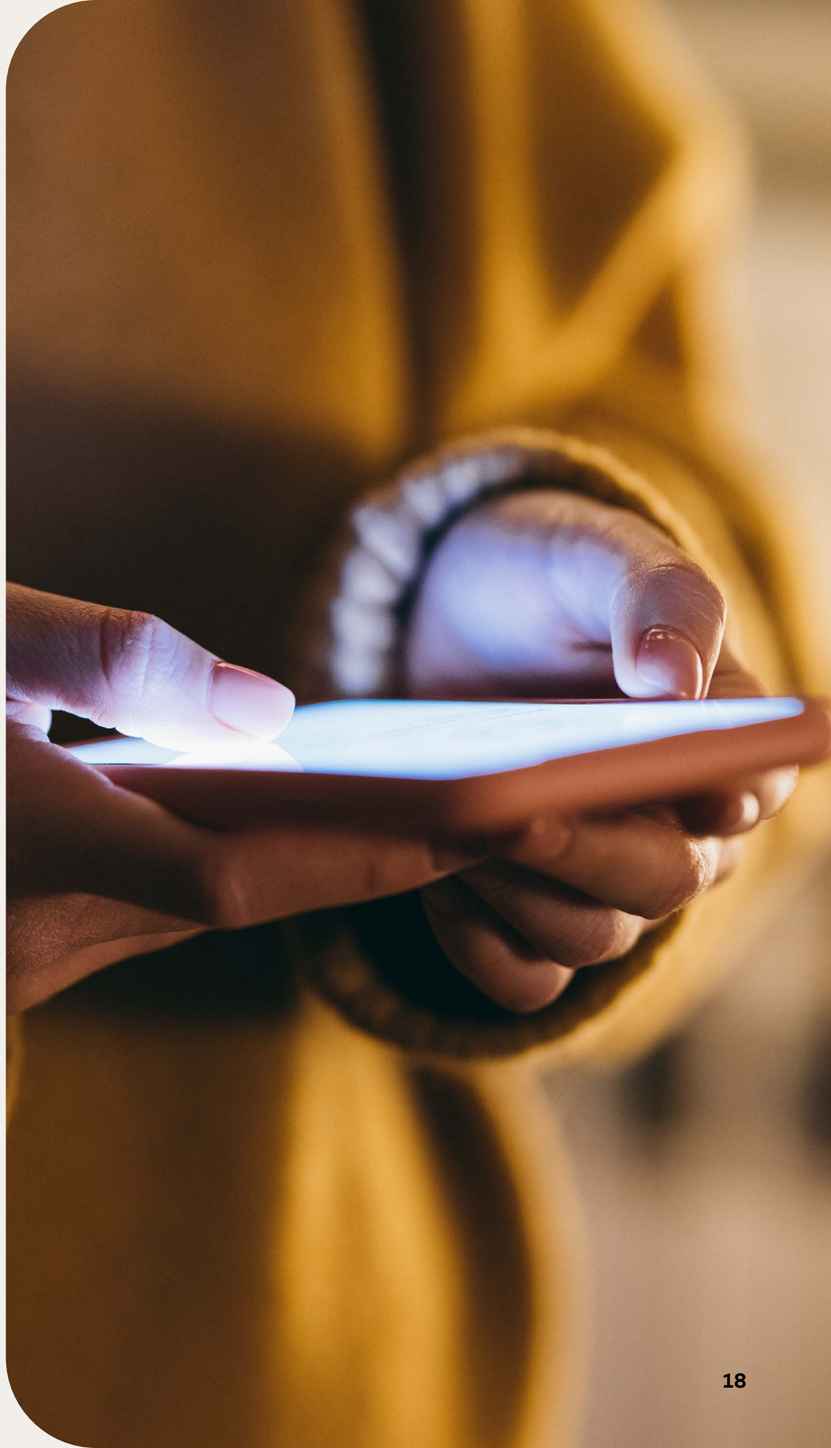
> *There are a number of external data sources that we can and should be tapping into ... it's about having the whole picture.*

Stuart Skinner
Head of The Fraud Prevention Team, NatWest

A critical component of fighting payment fraud is access to quality data that is properly integrated, safeguarded and used to create effective, robust and non-biased AI models.

Most respondents (64%) recognize that they need to accelerate the rate at which they acquire new, credible data sources in order to keep up with the evolution of payment fraud. Quality data sources allow financial services companies to uncover more context for each transaction and help businesses strengthen their defenses.

"The one thing that underpins everything is data," says NatWest's Skinner, who highlights the importance of intelligence sharing within and outside the finance sector. Third parties, such as big tech, telecoms or social media platforms, often see their services involved in payment fraud schemes. Any shared intelligence from these sources would help reveal where fraudulent attempts are taking shape. "There are a number of external data sources that we can and should be tapping into ... it's about having the whole picture," Skinner adds.

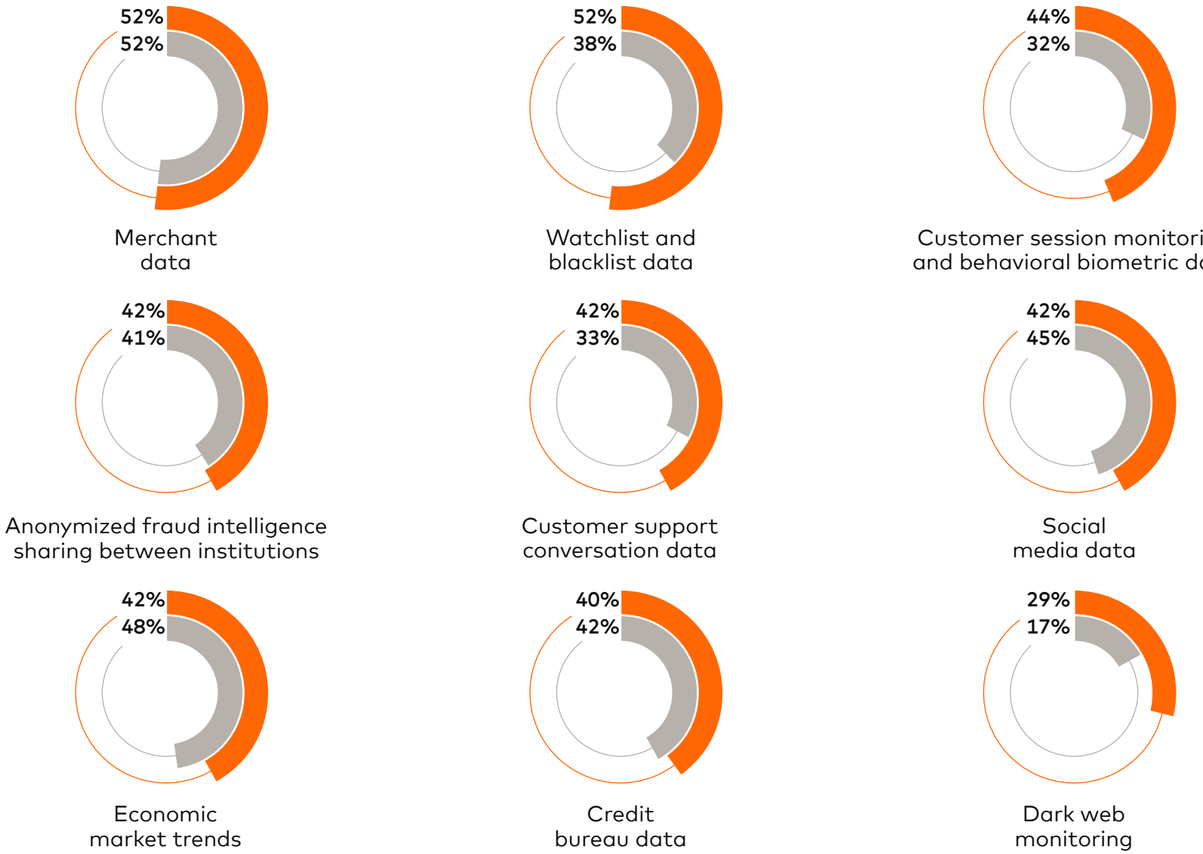


Overall, our survey respondents use merchant data (52%), economic market trends (47%) and social media data (44%) (Figure 10). This allocation is reflected in the non-leader group, too.

The leader group is as likely to use merchant data, but the group reports that watchlist and blacklist data are equally common data sources (52%), followed by session monitoring and biometric data from customers (44%). Anonymized fraud intelligence sharing between institutions is used by 42% of the leader group (Figure 10).

Figure 10

Overall sample comparison of datasets in current use and those considered most important for the next 12 months



Q: Which of the following datasets does your organization use for AI-powered fraud prevention activities?

Over the next 12 months, non-leaders are prioritizing data sources that the leader group is already using, such as customer session monitoring and behavioral biometric data, and watchlist and blacklist data. This indicates that the leader group is ahead of the curve in terms of data sources, and other organizations are just catching up.

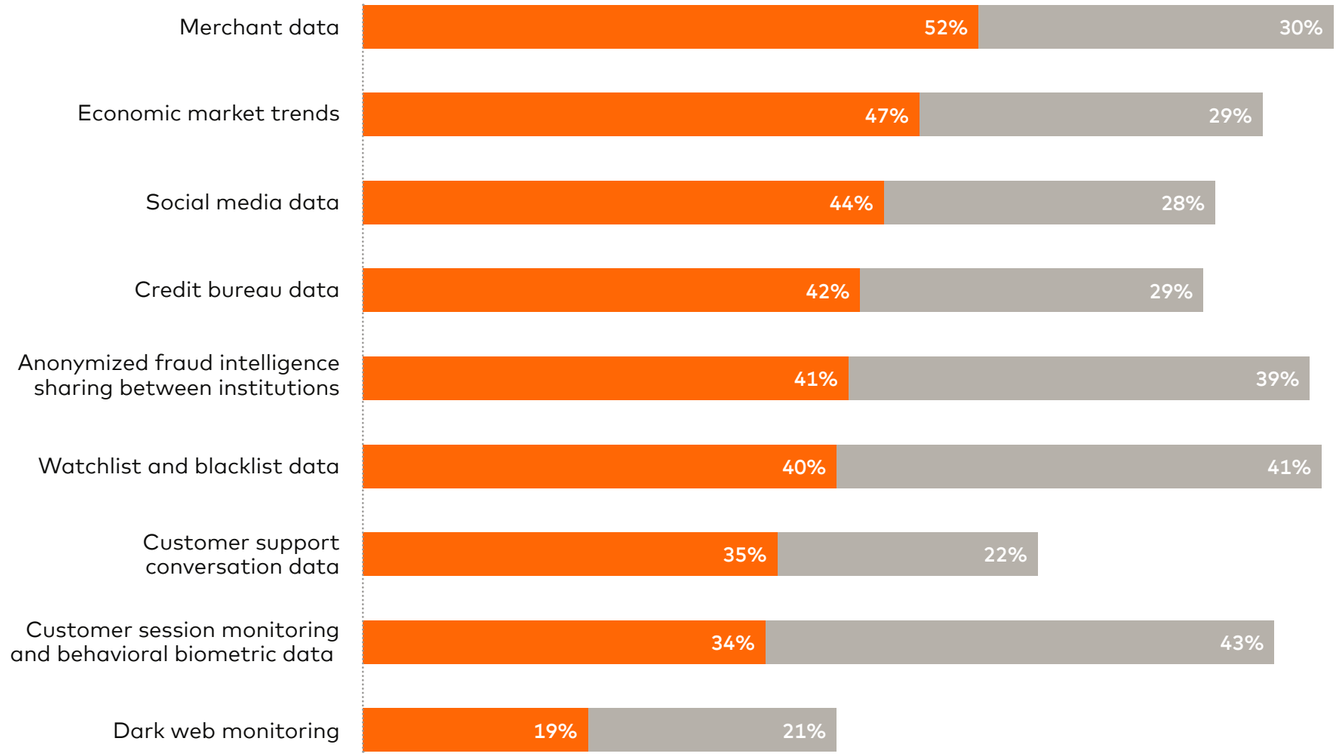
Behavioral biometrics — analyzing a user's unique patterns of interactions with devices and systems to verify their identity — is one of the most difficult use cases for organizations to employ against payment fraud. For instance, 28% of those surveyed say that they have yet to see returns on this use case (Figure 6).

In the year ahead, the prioritization of the current most popular data sources among the total sample (merchant data, economic market trends and social media data) will fall back, indicating a need for fresh data sources (Figure 11).

Behavioral biometrics is one of the most difficult use cases for organizations to employ against payment fraud.

Figure 11

Overall sample comparison of datasets in current use and those considered most important for the next 12 months



Q: Which of the following datasets does your organization use for AI-powered fraud prevention activities? And which, in your opinion, will be most important for achieving your organization's ambitions in the next 12 months?

Anonymization for better intelligence sharing

Gaining access to new supplies of credible data from external sources can be difficult. Data security and privacy rights can also present complexities. Cleber Martins, Global Head of Payments Intelligence and Risk Solutions at ACI Worldwide, highlights federated ML as a possible solution capable of detecting new fraud patterns as they emerge. Organizations in the payment journey can warn each other of suspicious behavior at their respective transaction stages without sharing any raw data.

"The messaging carries signals that AI can understand in exchange, but it doesn't expose the data behind it," says Martins. "Those signals can be expressed almost like a color [for instance, red for high risk, orange for medium risk]. But it doesn't carry any personal details or information behind it; it's almost like DNA."

ISO 20022 is an international standard for financial messaging that supports this process. It aims to create a common language and model for payment data, enabling interoperability between financial institutions.

> *"The messaging carries signals that AI can understand in exchange, but it doesn't expose the data behind it.*
>
> **Cleber Martins**
> Global Head of Payments Intelligence and Risk Solutions, ACI Worldwide

Data integration challenges

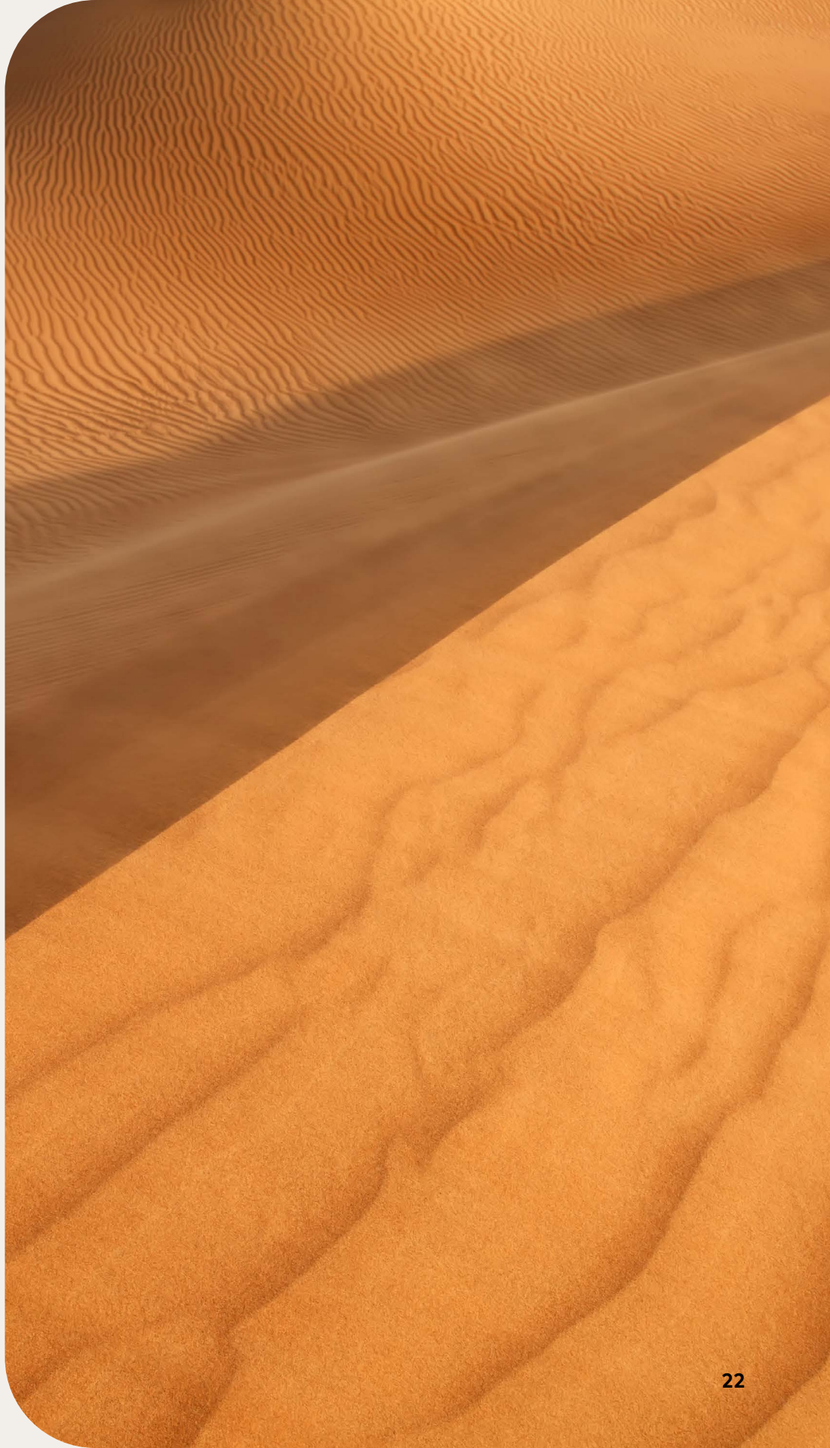
> *Like all banks, we've got an incredibly mature governance framework around how we do our modeling, what data goes in [and] how we ensure that we're comfortable with our data. Once you start going to external sources, that becomes more difficult.*

Stuart Skinner
Head of The Fraud Prevention Team,
NatWest

Once new data has been obtained, the next challenge is integrating it into AI systems effectively and accessibly, enabling interconnectivity across the payment ecosystem. Yet system and data integration issues are the toughest hurdles for organizations to overcome when using AI to combat payment fraud. Some 35% of respondents cite these as their main obstacles (Figure 8).

Data fragmentation and silos within the payment ecosystem, often caused by incompatible systems, mean organizations struggle to see the full picture on transactions. They impede their pattern detection and ability to understand the threat landscape.

"Like all banks, we've got an incredibly mature governance framework around how we do our modeling, what data goes in [and] how we ensure that we're comfortable with our data. Once you start going to external sources, that becomes more difficult," says NatWest's Skinner.



When business leaders tackle the data and system integration issues complicating AI programs, Mastercard's McGuigan advises that they take a balanced approach — one that addresses any near-term goals and immediate challenges while remaining aligned with the longer-term strategic integration goals that emphasize speed and agility.

A relative majority of respondents (48%) say they plan to address data integration issues in the next year by implementing processes to continuously update and retrain AI models (Figure 12).

Control group exercises can help troubleshoot AI models for data integration issues or integrity flaws that are undermining outputs.

Marnie Wilking, Chief Security Officer at Booking.com, says, "Control groups are vital for verifying AI outputs and retraining models." These methods involve running a portion of transactions through both AI and traditional or human-reviewed methods. "If the results differ significantly," Wilking adds, "you can investigate where the issue lies: whether it's the data sources feeding into the AI model, the model's learning sequence or potential AI bias."

Based on those findings, the business can decide quickly whether to reinforce or correct the model. "This is a continual, real-time feedback loop," says Wilking. "In areas where a model's decisions aren't yet trusted, those tasks can be allocated to humans. Then observations can be used to further train and improve the AI model."

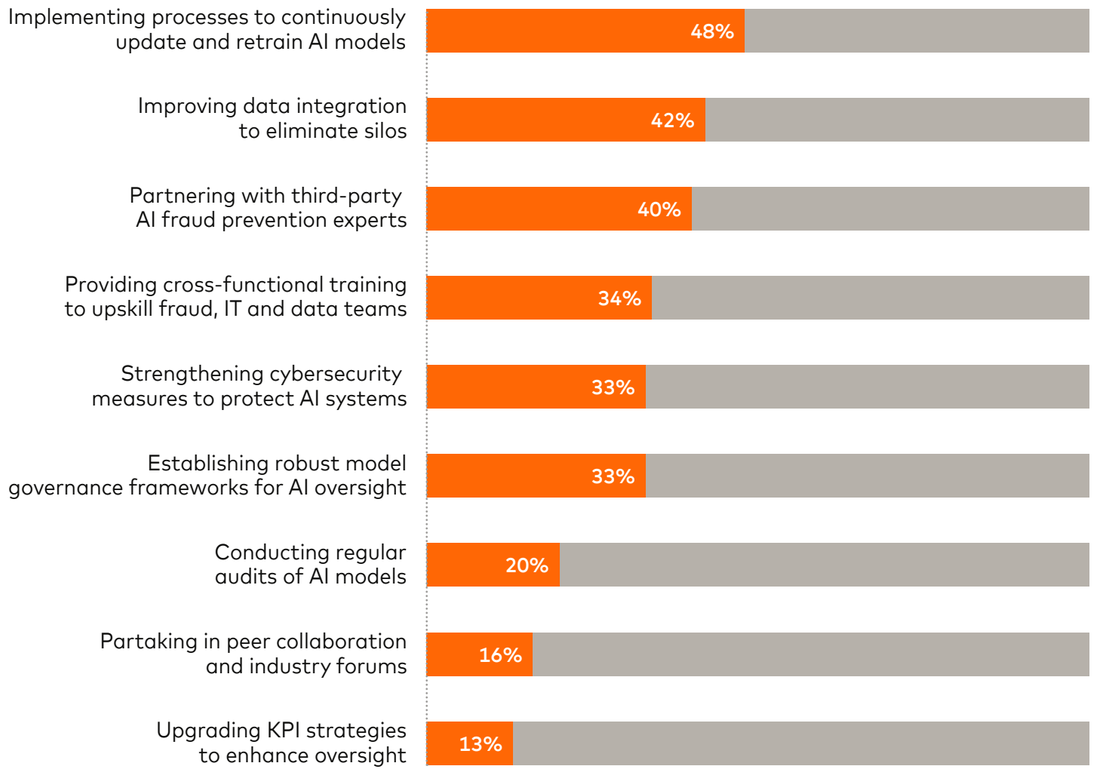
Payment companies say they will also prioritize improving data integration to eliminate silos (42%) and partnering with third-party AI fraud prevention experts (40%) (Figure 12).

48%

of respondents say they plan to address data integration issues in the next year by implementing processes to continuously update and retrain AI models.

Figure 12

Processes to update and retrain AI models and eliminate data silos are the top tactics for overcoming data integration issues in the next 12 months



Q: To overcome data integration issues, which of the following strategies will your organization need to prioritize in the next 12 months?

Maintaining data

Organizations are implementing data governance techniques to guarantee the quality, security and interoperability of data for AI fraud detection systems.

Data accuracy and integrity audits are the most popular governance tactic, with 50% saying they use them. Red teaming exercises — simulated cyberattacks — to test AI guardrails (45%) and AI explainability tools to review outputs (42%) are the next most popular governance tactics.

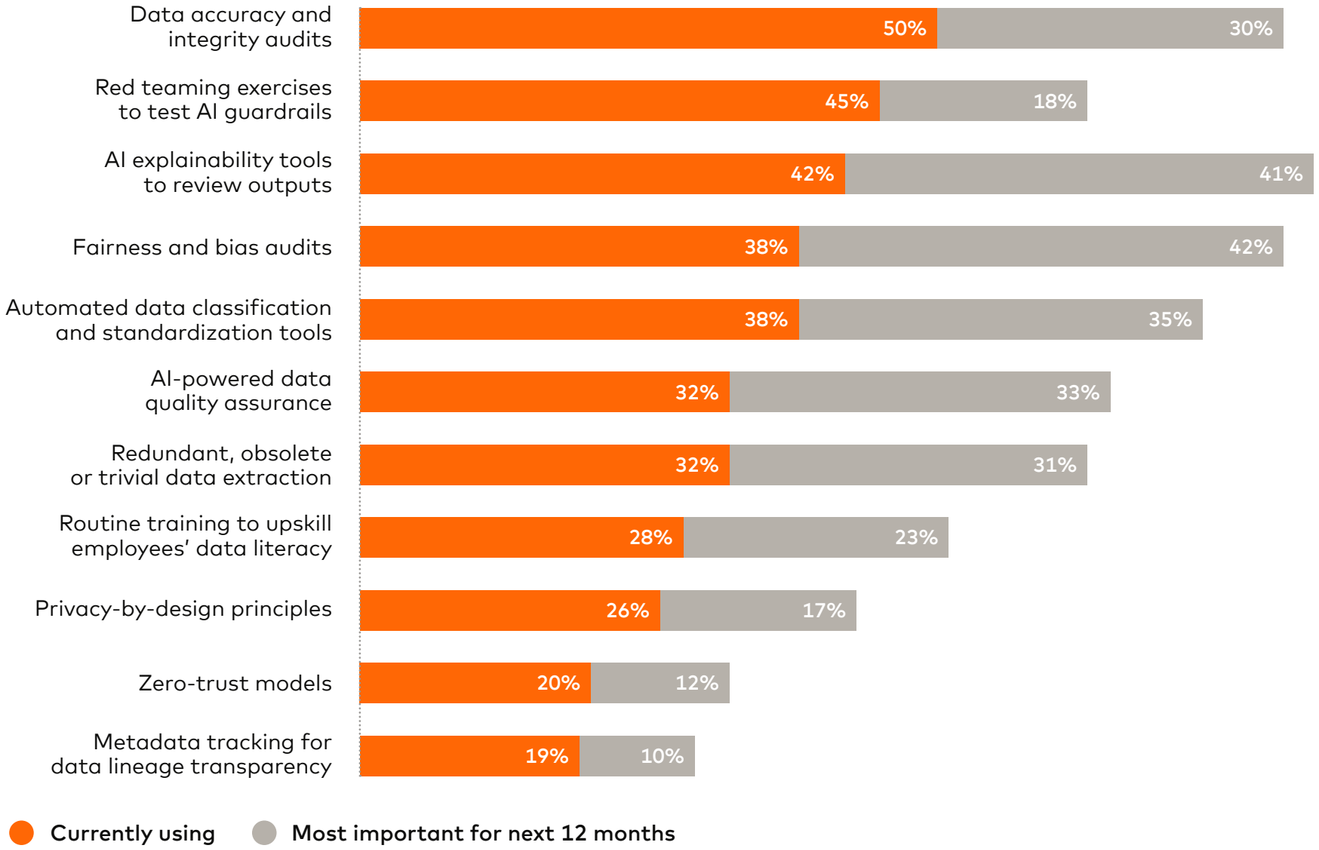
Looking ahead to the next 12 months, fairness and bias audits will become the top priority for respondents (42%). The leader group is already ahead of the game on this, naming fairness and bias audits as one of their top three governance techniques already in use. For the non-leaders, this places outside their top three (Figure 13b).

50%

Data accuracy and integrity audits are the most popular governance tactic, used by 50% of respondents.

Figure 13a

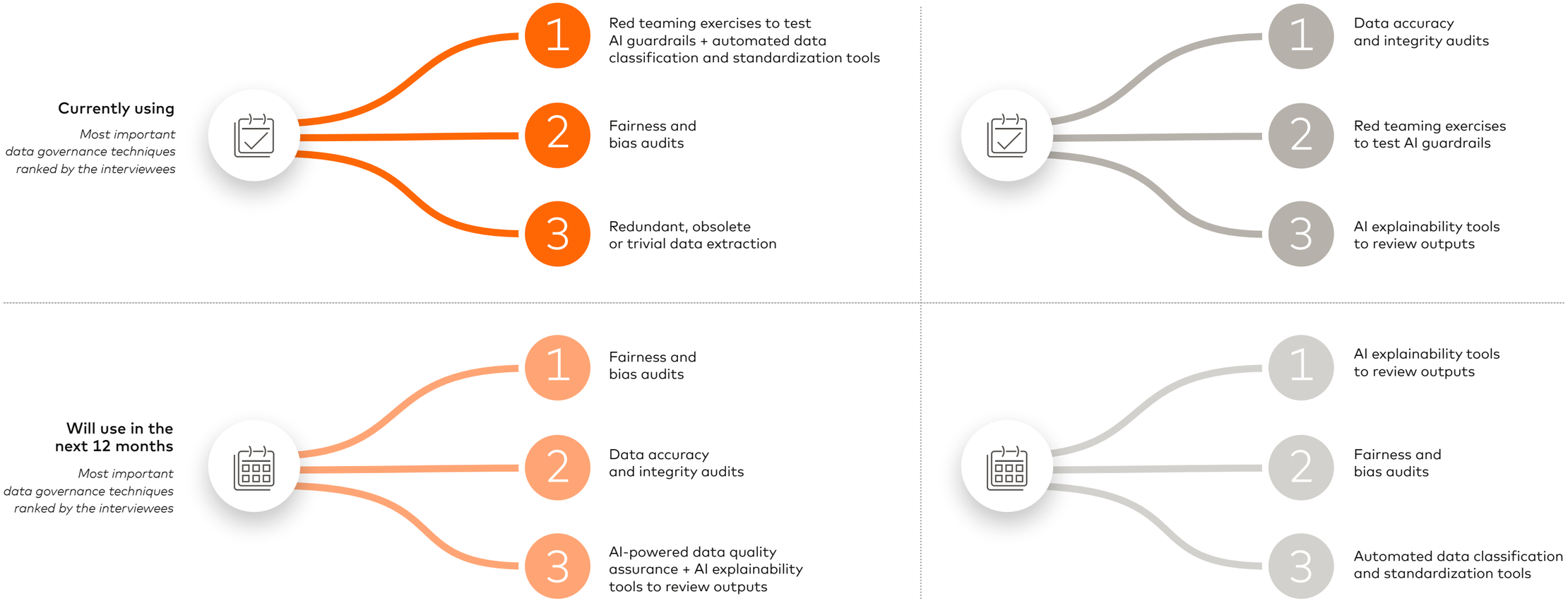
Overall sample comparison of data governance techniques in current use and those considered most important for the next 12 months for AI-powered fraud prevention activities



Q: Which of the following data governance techniques does your organization use currently for AI-powered fraud prevention activities? And which, in your opinion, will be most important for achieving your organization's ambitions in the next 12 months?

Figure 13b

Comparison of data governance techniques adopted by the leader group vs. the rest of the sample



Q: Which of the following data governance techniques does your organization use currently for AI-powered fraud prevention activities? And which, in your opinion, will be most important for achieving your organization's ambitions in the next 12 months?

Fairness and bias in data governance

Although AI is an effective tool in combating payment fraud, it is not a silver bullet. AI systems can be prone to bias and hallucinations.

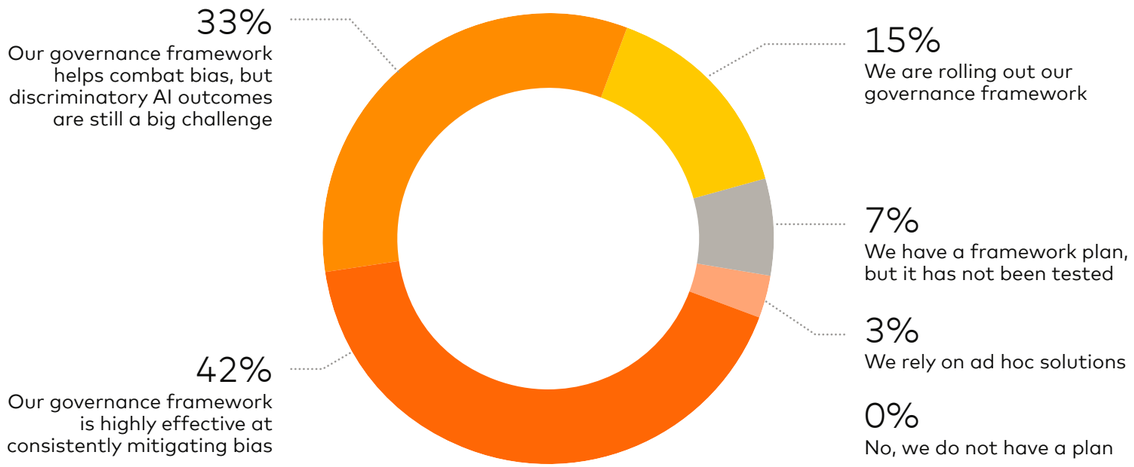
Bias can lead to discriminatory outcomes that undermine public trust in financial institutions. Biased models could incorrectly flag legitimate transactions as fraudulent, leading to unnecessary delays, account freezes and customer dissatisfaction and distress. They could also disproportionately target certain demographics or groups based on patterns in the training data, even if those patterns are not indicative of actual fraud. This could lead to discriminatory highlighting of transactions in certain geographies or with certain credit profiles, for example.

Three-quarters of survey respondents say they have a governance framework in place to address potential bias. Of these, 42% say their framework is highly effective. However, 33% say that while their framework helps, discriminatory AI outcomes are still present. Factoring in the respondents who do not yet have a framework in place or have not fully rolled one out, the research indicates that over half (58%) are at real risk of bias skewing their AI outputs or decision-making in fraud prevention activities (Figure 14).

Our research confirms that as the industry adapts to the evolving payment fraud landscape, alliances and anonymized fraud intelligence sharing will be crucial.

Figure 14

Most organizations have some form of anti-bias AI framework, but AI discriminatory outcomes are still a threat for many



75% have rolled out an anti-bias AI framework.

58% are at higher risk of AI biases skewing outcomes.

25% have not yet rolled out an anti-bias AI framework.

Q: Do you have a robust model governance framework in place to address potential bias in your AI payment fraud prevention outcomes?

04

A united front gives better payment protection

Building alliances

Combating fraud is a collective endeavor. By sharing intelligence, organizations have a more comprehensive view of transactions and the threat landscape, making it easier to spot patterns and stop schemes at the source.

"We believe strongly in sharing intelligence. A rising tide raises all boats," says Wilking of Booking.com. "It strengthens the security posture of the whole industry by boosting awareness of new threat vectors and the warning signs to look for. The more we can help each other improve, the more it also helps the smaller businesses that might not have the resources that some of the big companies have."

In addition to supporting other organizations battling the same issues, collaborating with other businesses creates a united front and a stronger opposition against fraudsters, Wilking explains. "Instead of [just] Booking.com or Expedia or Hyatt going to law enforcement agencies, we can do it as a collective and bring all the data together to say, 'Here's how many companies are impacted; we're all seeing the same threat actors.' Law enforcement wants that information."

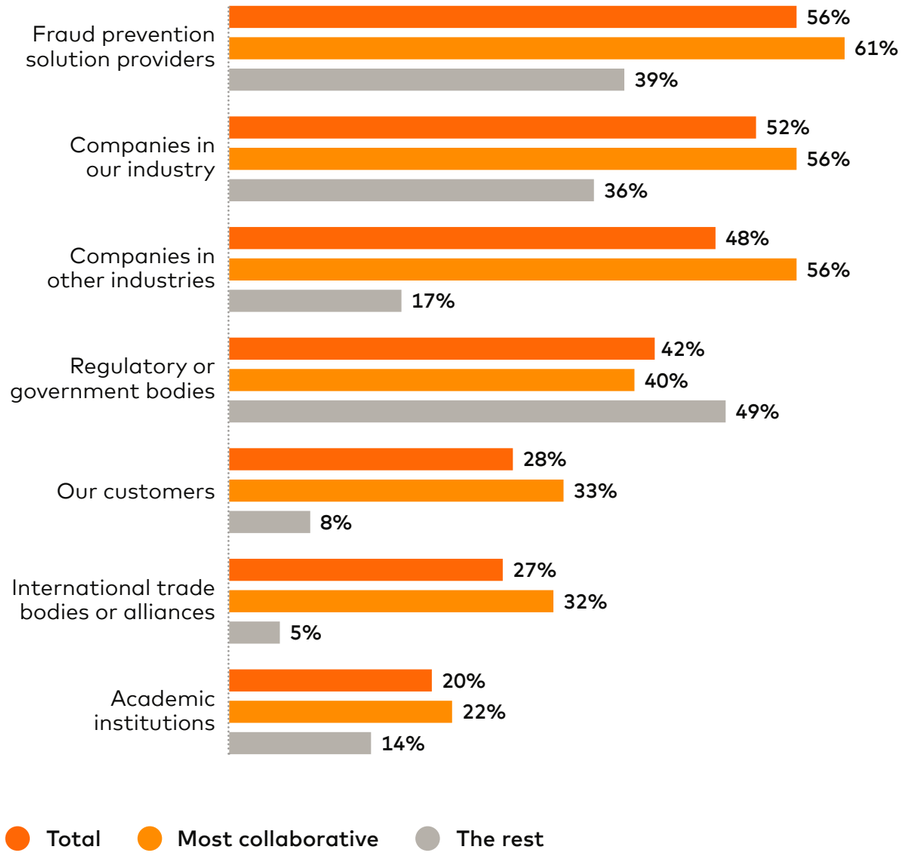
Most survey respondents (59%) agree that forming external alliances focused on intelligence sharing is crucial. Our leader group maintains that partnerships will be their main solution to tackling evolving fraud.

The most popular collaborator type for payment industry organizations is fraud prevention solution providers (56%), followed by companies in the same industry (52%) and companies in other industries (48%).

> *"We believe strongly in sharing intelligence. A rising tide raises all boats.*
>
> **Marnie Wilking**
> Chief Security Officer,
> Booking.com

Figure 15

Entities that organizations in the payment industry collaborate with to combat payment fraud threats



Q: What entities does your organization collaborate with to combat payment fraud threats?

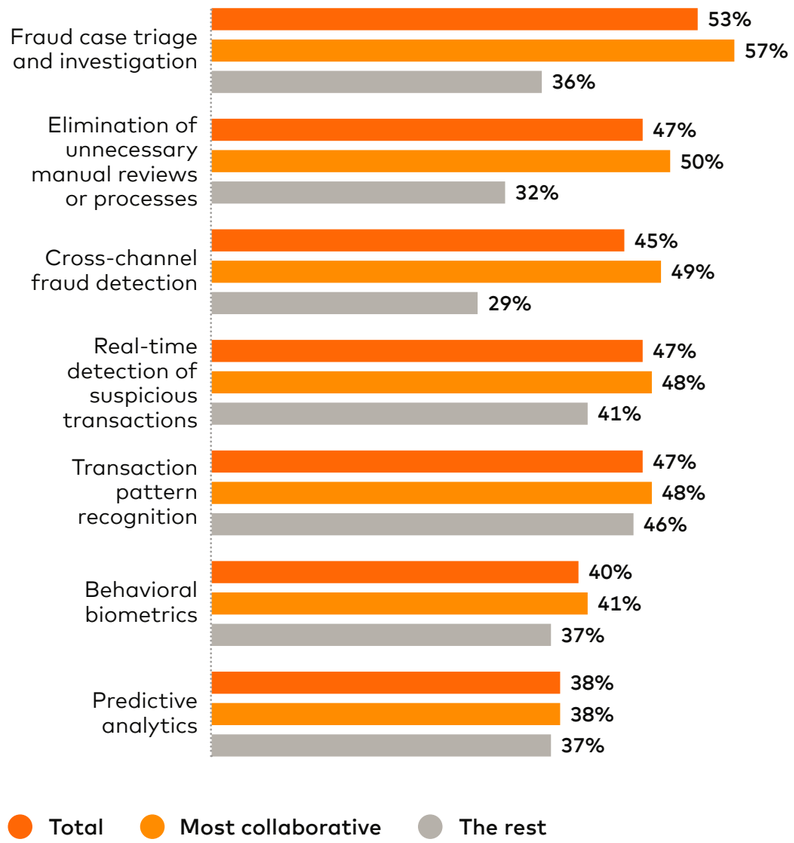
According to our research, those companies that collaborate with a greater variety of entities are more likely than less collaborative firms to see high returns from their AI use cases. Fraud case triage and investigation is particularly fruitful: 57% of the most collaborative firms say they are seeing high returns from this AI-powered use case compared with just 36% of the rest. And 49% of the most collaborative companies see high returns from cross-channel fraud detection, compared with 29% of the rest (Figure 16).

57%

of the most collaborative firms are seeing high returns from AI-powered fraud case triage and investigation.

Figure 16

In the majority of AI fraud prevention use cases, more collaborative firms are more likely to see success than their counterparts



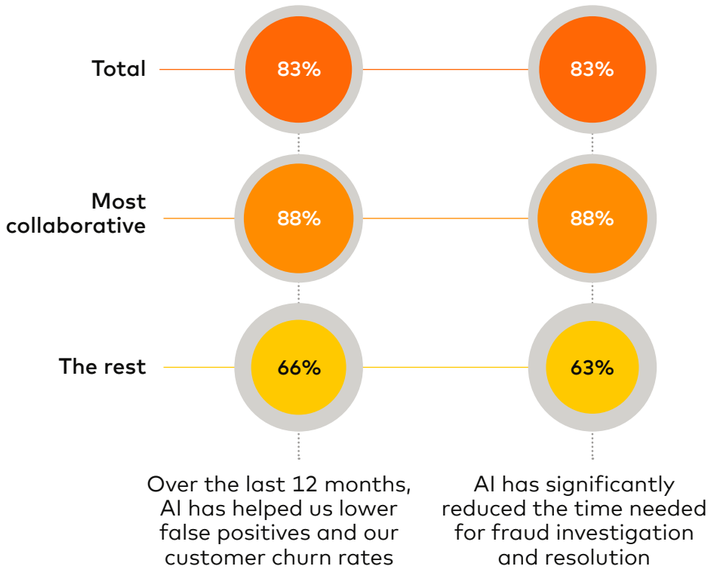
Q: How effective are your organization's AI-powered fraud prevention activities in the following areas? (Chart shows those seeing high returns)

The most collaborative firms are also more likely to say that AI has significantly accelerated fraud investigation and resolution times and that, over the past 12 months, AI has helped them lower false positives and customer churn rates.

In addition to responding more effectively to fraud cases, more collaborative firms demonstrate a broader awareness of the threat landscape. They are more likely to expect a larger range of fraud tactics to become an increasing threat in the coming 12 months. Most notable are impersonation schemes, which 66% of greater collaborators expect to increase in the next year, compared with 37% of less frequent collaborators.

Figure 17

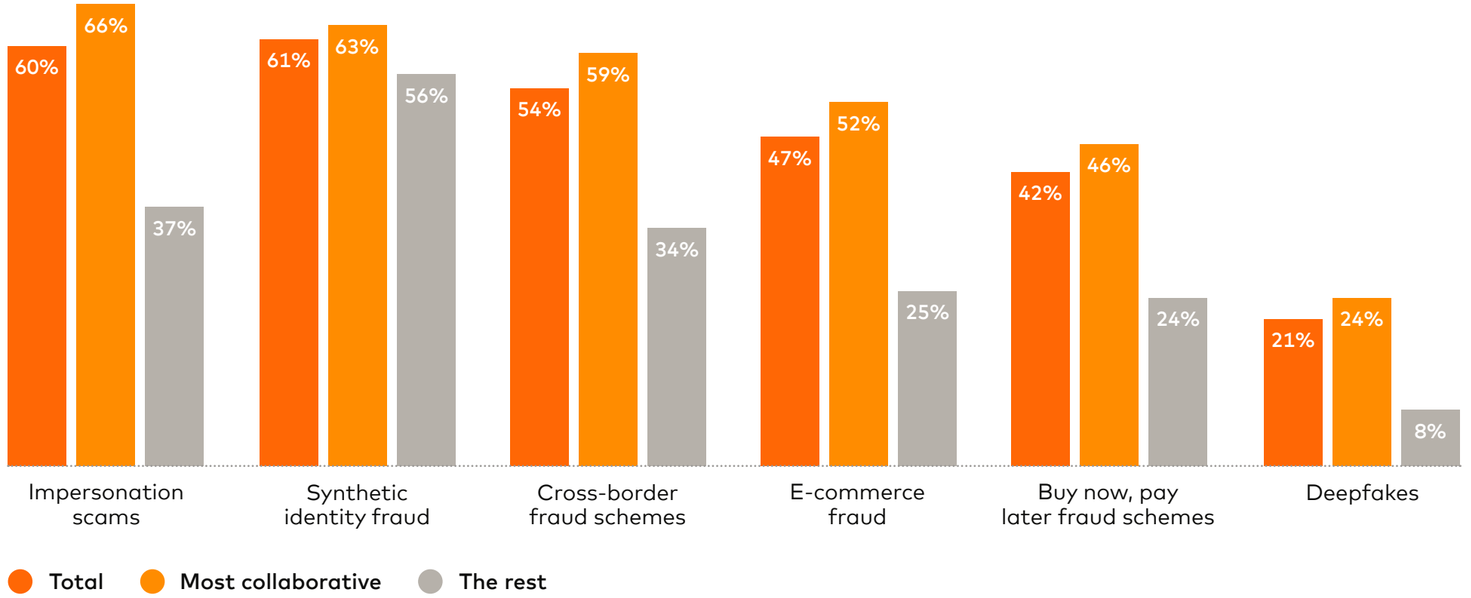
More collaborative firms are more likely to have used AI to accelerate fraud investigation times and lower false positives



Q: Please indicate whether you agree or disagree with the following statements.

Figure 18

More collaborative firms have a more detailed view of the threat landscape



Q: Which of the following, if any, do you foresee becoming an increasing threat over the next 12 months?

05

Closing remarks

The proliferation of payment channels has increased the number of entry points and vulnerabilities that fraudsters can exploit. Payment industry executives expect the frequency and sophistication of fraud attacks to increase in 2025. Recent reports of targeted CEO impersonation schemes, which aim to steal sensitive information from employees, and Gen AI-enhanced investment schemes targeting wealthy investors, are further fueling concerns.

But payment companies are making progress backed by ever more powerful AI tools. Benefits and ROI are accumulating as models mature and become more sensitive and highly attuned.

Looking ahead, greater collaboration and cohesion will be critical to maintaining a united front against the ever-evolving threat of payment fraud. "AI systems need to be integrated into every part of an organization," says Martins of ACI Worldwide, "not just a project here and there." By embracing AI, leaders can make sure that crucial data is shared throughout the organization and used optimally for tackling payment fraud, as well as in other critical business processes. This, explains Martins, will reduce fraud losses and, ultimately, increase revenue.

"That democratization of domain knowledge expertise across the organization will increase operational efficiency for everyone," says Martins. "This is a whole change of perception; it's AI as a framework, not as a loop."

Organizations must look beyond the confines of their businesses to collaborate and share information across industries, explains Wilking of Booking.com. "It's a trust ecosystem," she adds, noting initiatives such as the European Union's Information Sharing and Analysis Centers, which enable confidential and anonymized information sharing about cyber threats and fraud trends.

With greater collaboration and intelligence sharing comes power. Together, organizations, supported by the latest AI technology, can create a defensive wall that even the most agile cyberfraudsters will find challenging to scale.

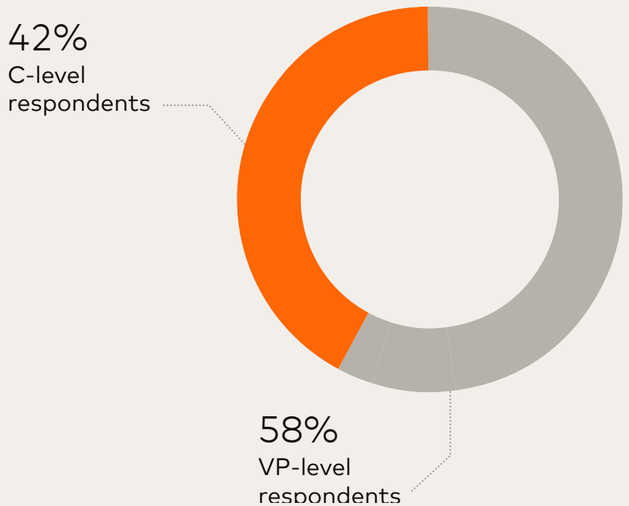
> *"That democratization of domain knowledge expertise across the organization will increase operational efficiency for everyone.*

Cleber Martins
Global Head of Payments, Intelligence and Risk Solutions, ACI Worldwide

06

Methodology

About the total sample of respondents



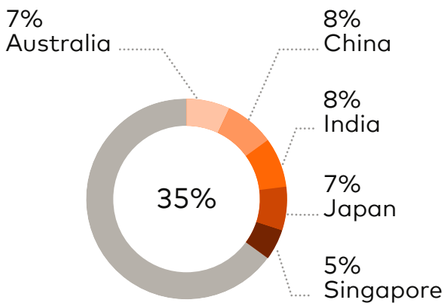
The business leaders surveyed are from various parts of the payment industry: issuing banks, acquiring banks, payment facilitators, payment processors, merchants/retailers and digital wallet providers.

The entire sample is composed of senior leadership, with 42% at the C-level and 58% at the vice president (VP) level. The organizations they work for generate annual revenues above $50 million.

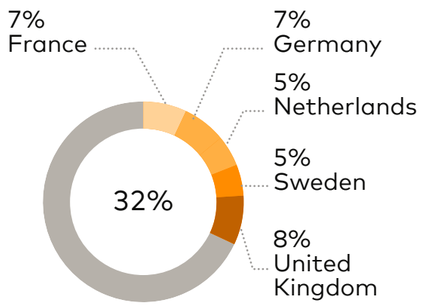
In addition to the survey research, we conducted one-on-one interviews with several senior executives and experts, and insights from these are featured in this report. Our thanks go to everyone who contributed.

This study is based on a survey of 300 executives from 17 countries:

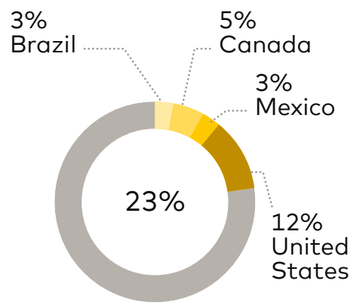
Asia Pacific



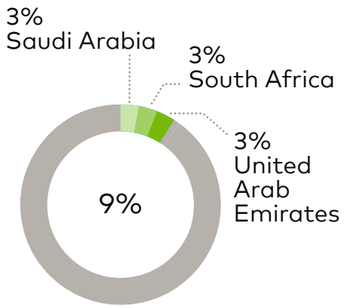
Europe



Americas



Middle East and Africa



Note: These figures have been rounded for clarity. The figures add up to 99% due to rounding.

FT LONGITUDE