ALLOY

2025

State of Fraud Report

Fraud trends and predictions, according to US decision-makers

How did fraud affect financial institutions and fintechs in 2024?

60%

experienced an **increase in fraud attacks** affecting consumer and business accounts.

56%

reported catching fraud most commonly **at the time of the transaction**, while only 33% indicated that they detect fraud most commonly at onboarding.

71%

found **financial criminals and fraud rings** to be the main culprits behind fraud attacks.

93%

agreed that **machine learning and generative AI** will revolutionize fraud detection.

Table of contents

About the survey

About the survey

Methodology

We surveyed **486 industry leaders** at financial organizations that spanned enterprise banking, mid-market banking, and fintech.

Respondents held a director-level position or higher.
Their titles related to:

- Risk/compliance
- IT/security
- Digital banking
- Fraud
- Operations
- Product management
- Internal Audit

This survey ran from **October 2 - 28, 2024**, and was conducted by The Harris Poll, an American market research and analytics company since 1963.

Respondent breakout by financial sector

Respondents identified their organization as one of the following:

Enterprise banks (32%)

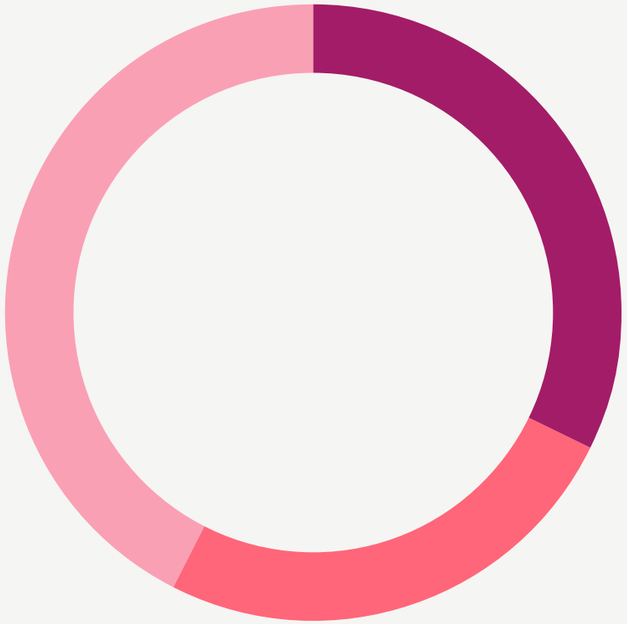
Includes enterprise banks.

Mid-market banks and credit unions (25%)

Includes mid-market banks, regional banks, and credit unions.

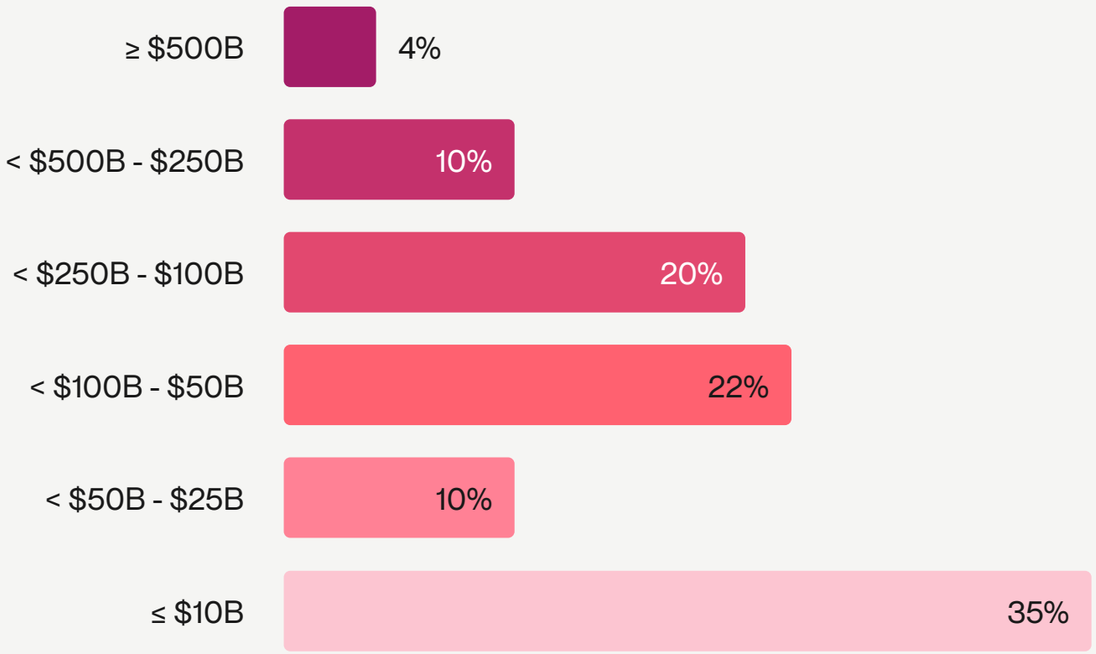
Fintech (42%)

Includes fintechs and online/ pure-play lending institutions.



Firmographics

Assets



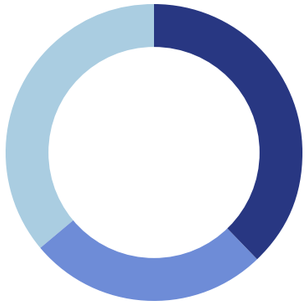
Respondents only reported assets if they identified as working at banks or credit unions. Fintech assets were not recorded.

Size by employee count

Respondent demographics

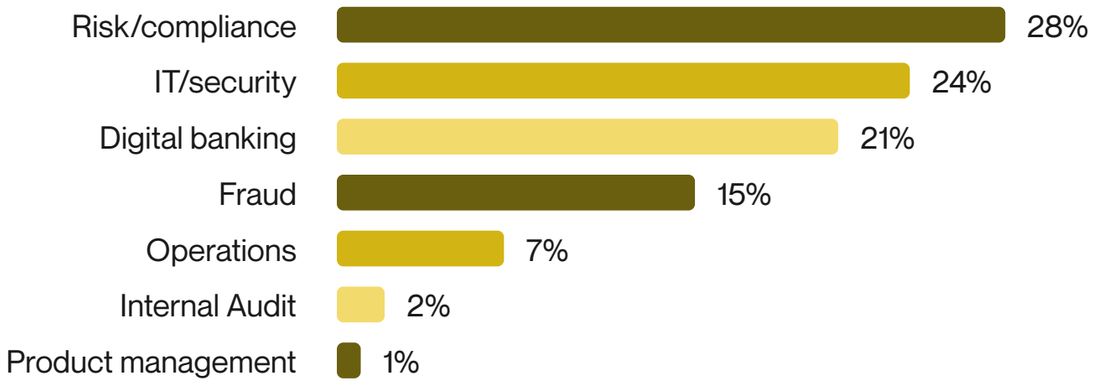
Job position

Respondents had to be at least a director at their organization.



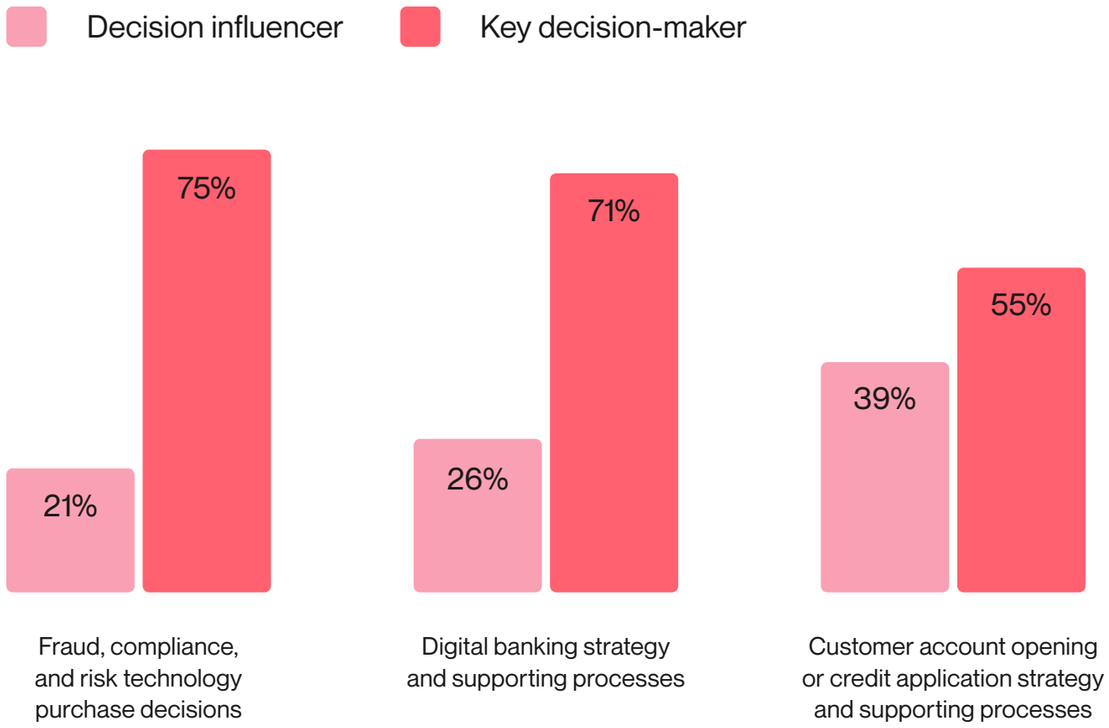
- C-level executive (38%)
- Vice president (26%)
- Director (36%)

Department



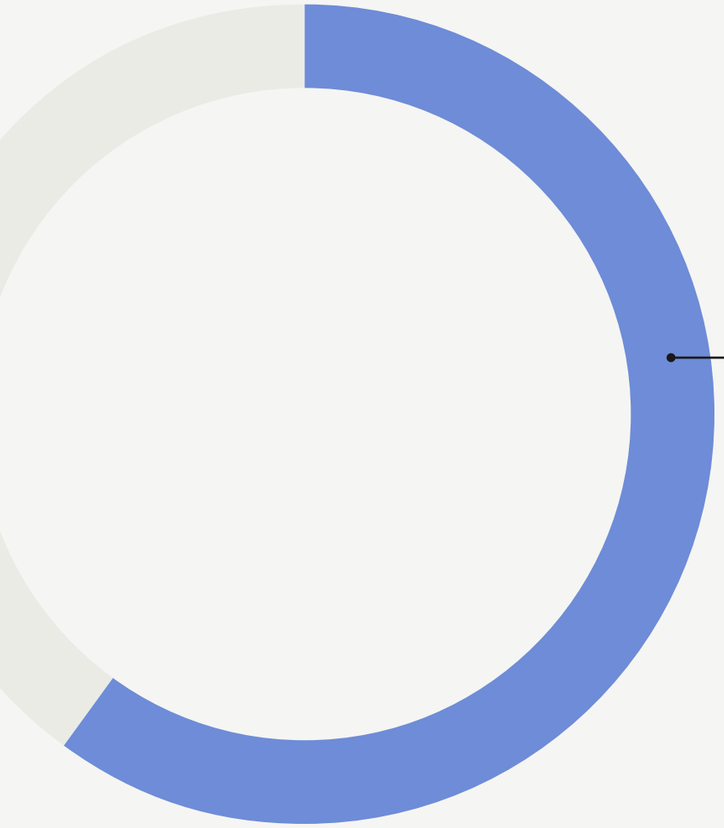
Decision-making authority

Respondents were influencers or key decision-makers in at least one fraud-related category.



Key findings

Fraud continued to rise in 2024 at a steady rate.



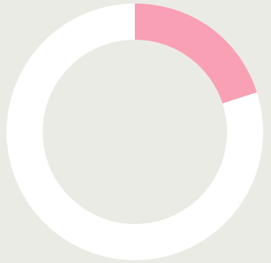
60%

of financial institutions and fintechs said fraud grew across consumer and business accounts in the last year.

Fraud was most common on digital channels, with **80%** of fraud events occurring on online or mobile banking channels.

The leading fraud types were:

1. Credit card fraud
2. Account takeover (ATO) fraud
3. Identity theft



20% of enterprise banks rank check fraud as their most common fraud type.

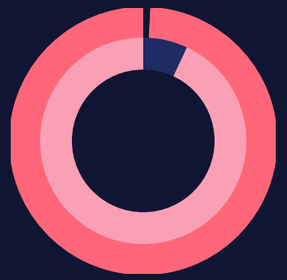
31% of organizations faced total fraud losses exceeding $1M.

Trending themes in fraud

Industry leaders are focused on AI, identity, and fraud damages — both reputational and monetary alike.

AI hype becomes reality

AI is no longer just a tool for bad actors.



99%

of financial organizations said they **currently use AI in the fight against fraud.**

93%

agreed that machine learning and generative AI will revolutionize fraud detection.

Costs of fraud keep climbing

Organizations continue to experience significant fraud losses.

31%

of financial organizations lost over $1M to fraud in 2024.

72%

ranked financial loss and client attrition as among the worst impacts.

73%

considered reputational damage to be the most severe fraud consequence.

Identity is central for fraud prevention

Leaders are turning to more sophisticated and agile technology to understand customer identity and keep up with evolving fraud tactics.

1 in 3

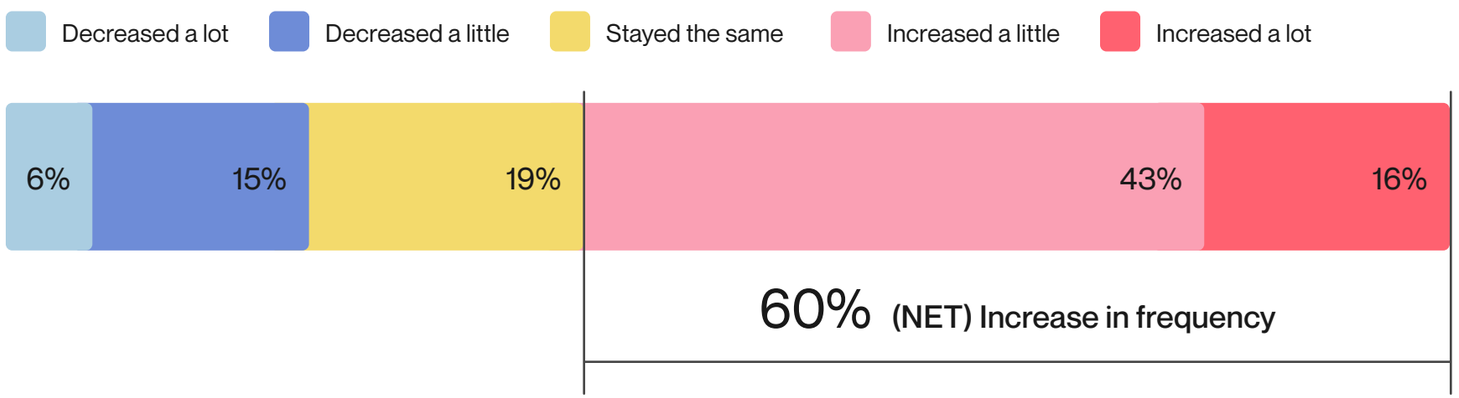
financial organizations said that implementing an identity risk solution has had the greatest impact on reducing fraud rates at their organization.

The current fraud landscape

60% of financial organizations reported an increase in fraud events affecting consumer and business accounts.

How has the frequency of attempted fraud events changed compared to last year?

Consumer & business accounts

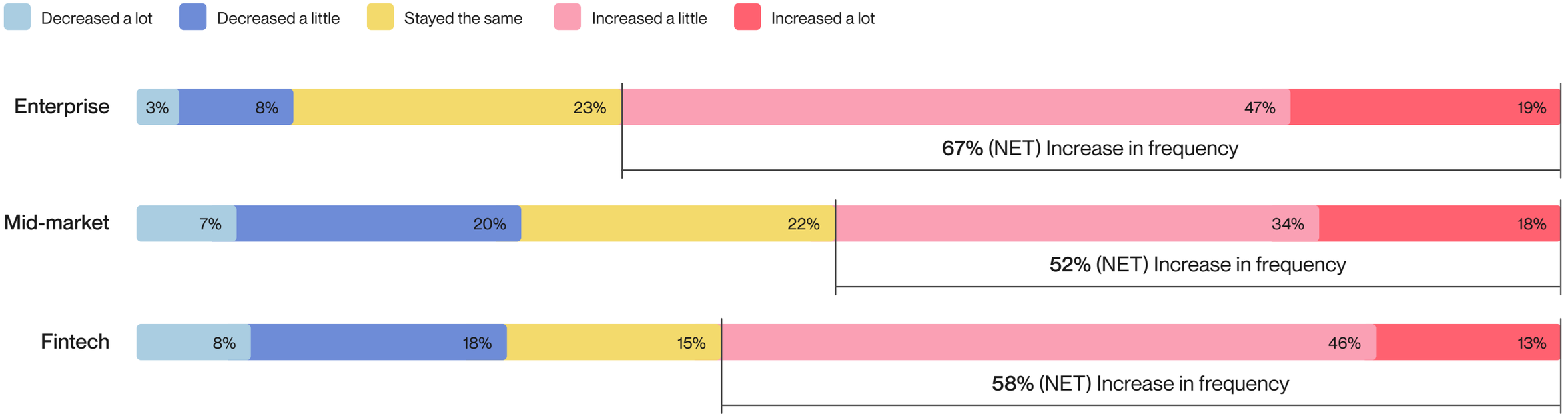


The survey defined a “fraud event” as an effort to exploit a vulnerability in an organization’s fraud controls, and/or deliberate deception of the organization, consumer, or business for financial gain.

Enterprise banks experienced the most fraud growth, with nearly 70% reporting a rise in fraud.

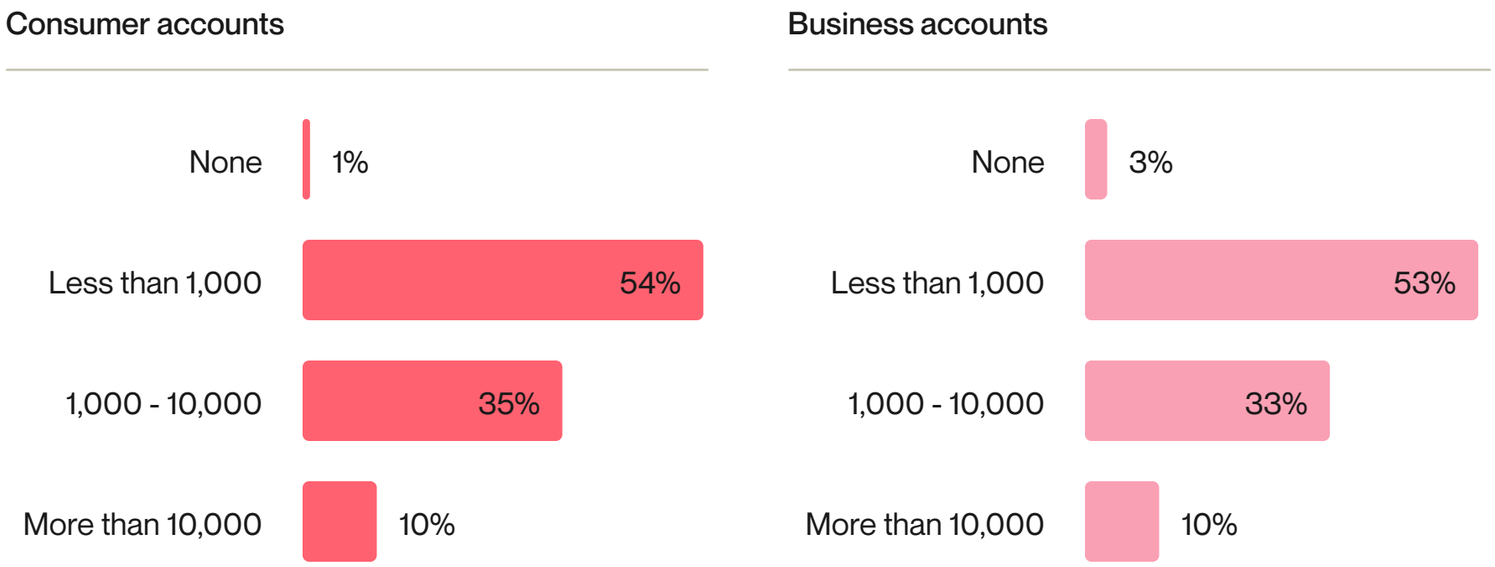
How has the frequency of attempted fraud events changed compared to last year?

Consumer & business accounts



Consumer accounts faced slightly more fraud events than business accounts in 2024.

How many consumer/business accounts at your company have exhibited fraud in the past year?

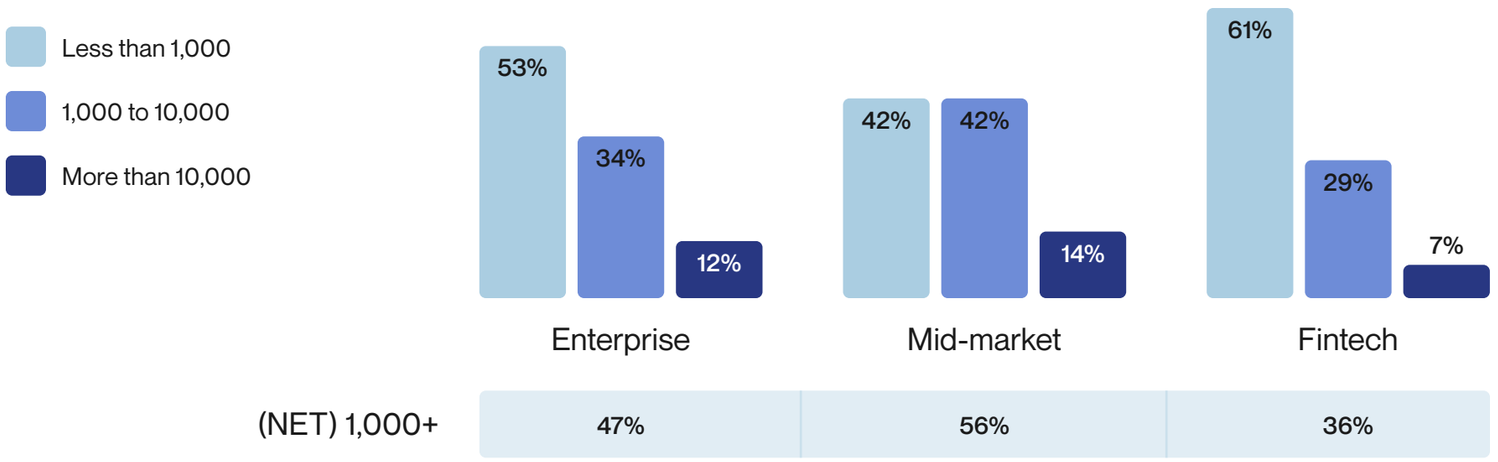


45% of respondents reported that 1,000+ consumer accounts were subject to fraud attempts, as opposed to **43%** of respondents reporting that 1,000+ business accounts were subject to fraud attempts in the past year.

Mid-market banks reported the highest levels of fraud on average. 56% of mid-market banks reported over 1,000 fraud cases — higher than any other sector.

How many consumer/business accounts at your company have exhibited fraud in the past year?

Consumer & business accounts



Alloy insight

Mid-market institutions reported a higher incidence of fraud compared to enterprise banks and fintechs, which is surprising and may indicate discrepancies in reporting methods.

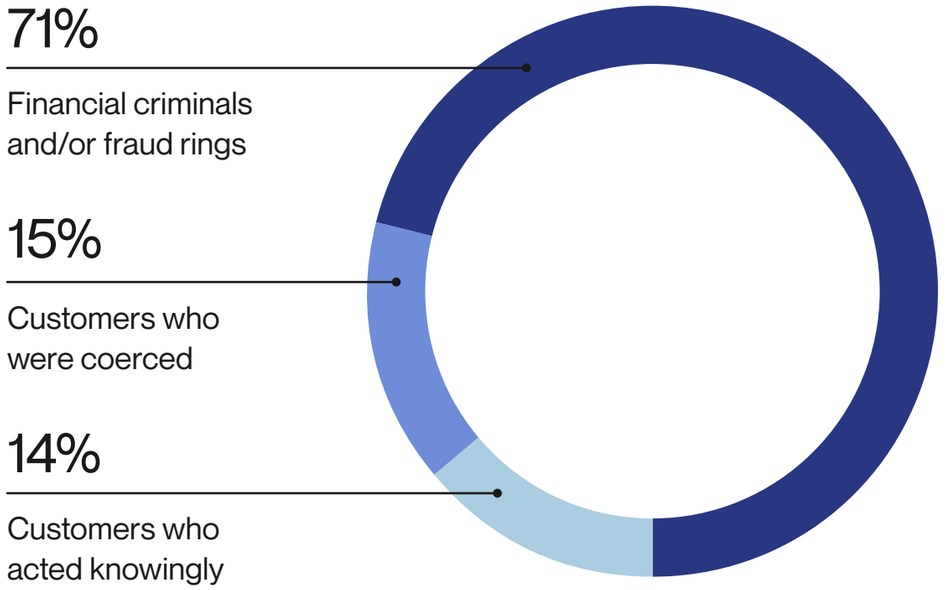
For example, enterprise organizations might only report accounts where SARs were filed, cases requiring closure, or incidents tied to closed accounts.

Alternatively, enterprise banks may be perceived to have better fraud controls than smaller financial institutions, causing them to be targeted by fraudsters less frequently.

Respondents overwhelmingly agree that sophisticated fraud groups are responsible for the majority of fraud at their organization.

Decision-makers reported near-equal volumes of first-party fraud (customers knowingly committing fraud) and scams (customers being coerced into committing fraud).

Who did your organization determine was responsible for the majority of attempted fraud events at your organization in the last twelve months?



Alloy insight

In past editions of this report, first-party fraud was often ranked among the top fraud types reported by financial institutions and fintechs. Today, decision-makers at financial organizations say that most fraud attempts originate from criminal groups, marking a shift in fraud attribution from first to third-party actors.

While attributing more fraud to financial crime rings may seem grim, in reality, it isn't. To conduct systematic fraud attacks, these bad actors use a replicable pattern to scale their activities. Financial organizations can teach those fraudulent patterns to machine learning algorithms, using AI to help alert them to when a fraud attack is happening.

When fraud prevention coverage is applied widely enough across the industry, the cost of committing fraud goes up. As a result, crime rings are driven out of business.

Insight from

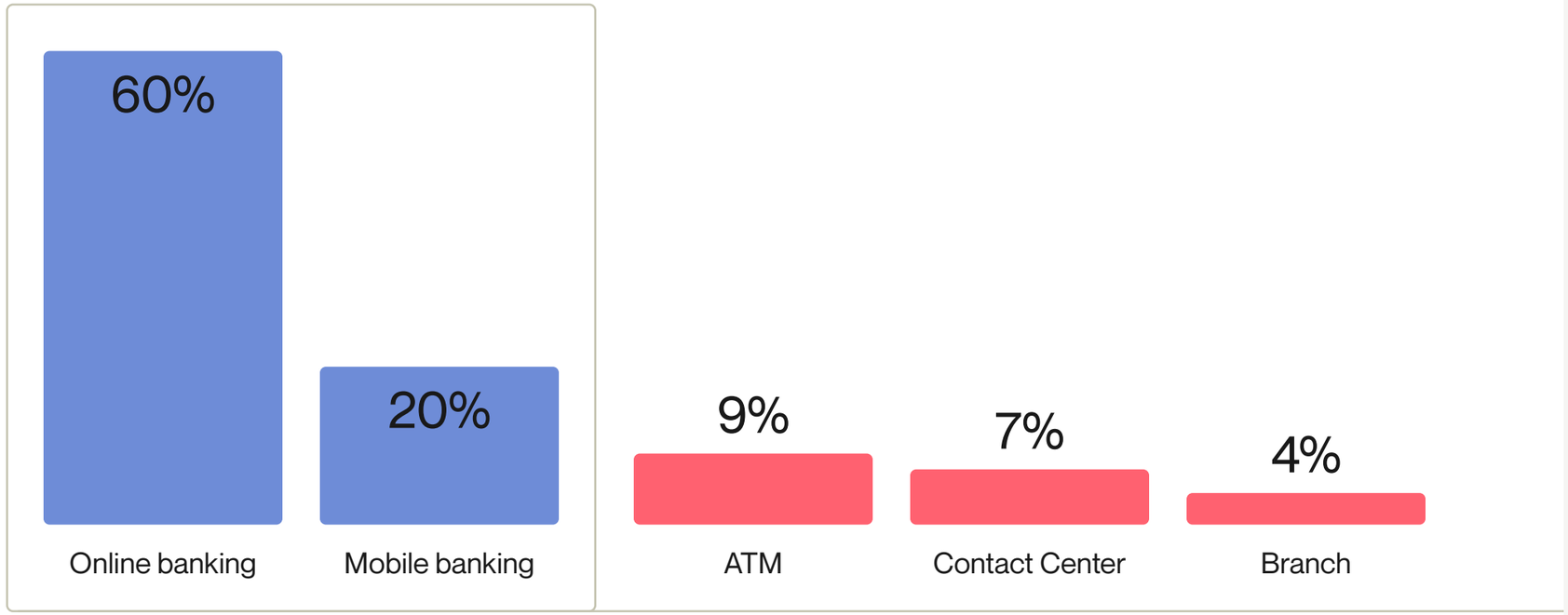
Trace Fooshée

Strategic Advisor at **Datos Insights**

"Many fraud executives have expressed concern that the low barriers to entry associated with check fraud and authorized payment scams coupled with the pervasive perception of economic uncertainty that began with the pandemic, but that stubbornly persists today, has created the ideal conditions for expanding the ranks of both 'citizen fraudsters' and organized crime rings."

Despite equal investment in physical and digital fraud prevention, more fraud occurred in online and mobile banking than any other channel.

On which channel did fraud events occur most frequently at your organization in the last twelve months?

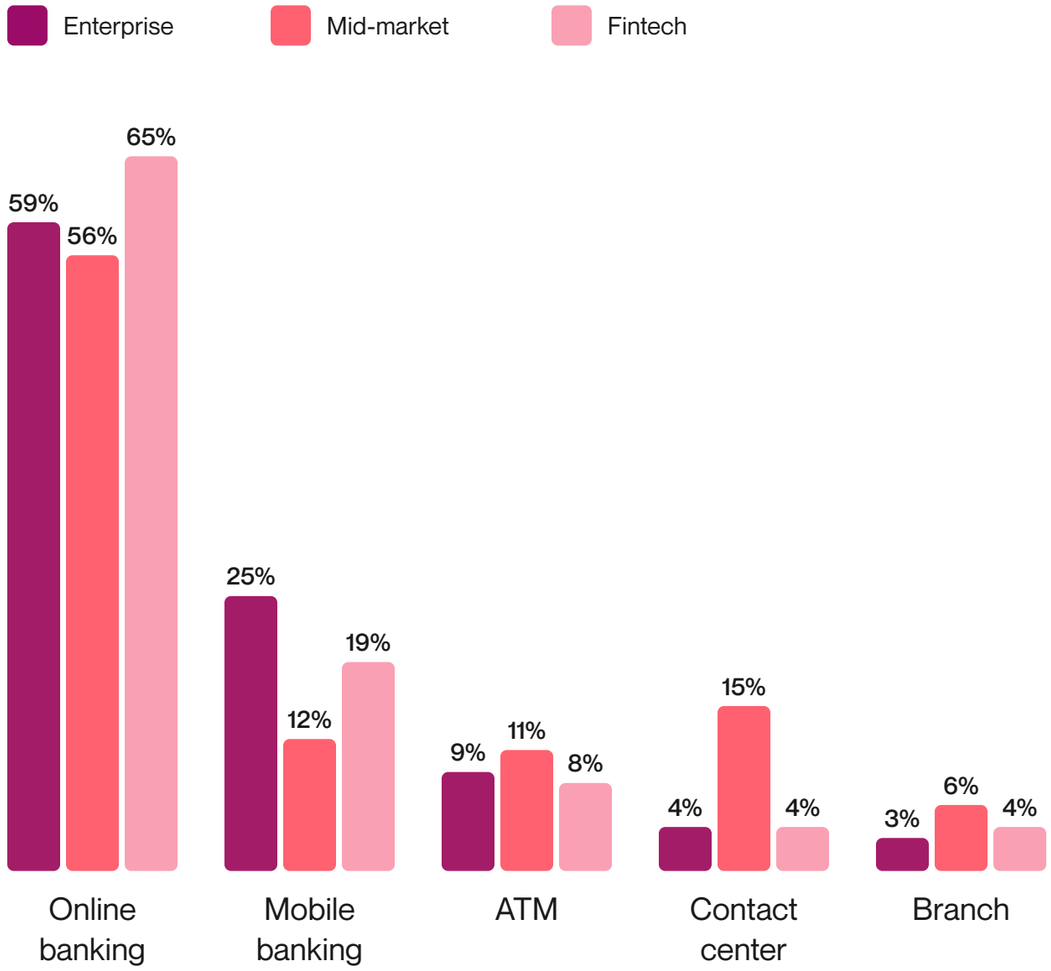


90%

of respondents agreed that their organization invests just as much time preventing fraud **in-branch** as it does on **digital channels**.

Unlike other sectors, mid-market banks and credit unions noted more fraud events in contact centers than mobile banking apps.

On which channel did fraud events occur most frequently at your organization in the last twelve months?



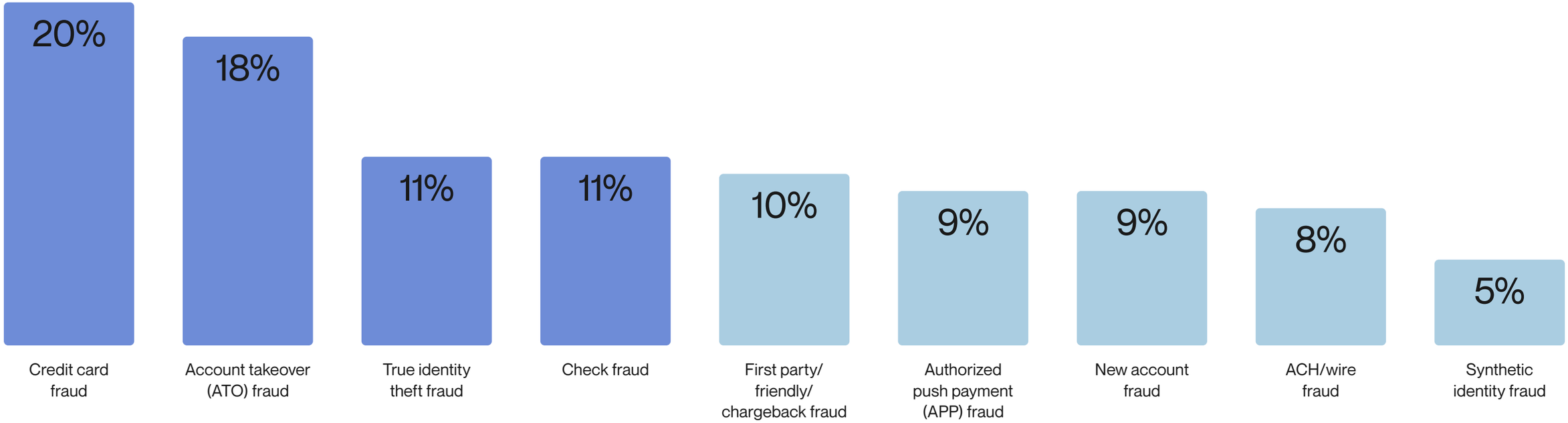
Alloy insight

These results indicate that most financial organizations categorize fraud based on how the funds leave their system, which is why online and mobile banking channels are credited with the most volume.

If more organizations tracked fraud based on its point of origin, in addition to how funds exited the organization, we could gain clearer insight into shifting fraud channels and patterns.

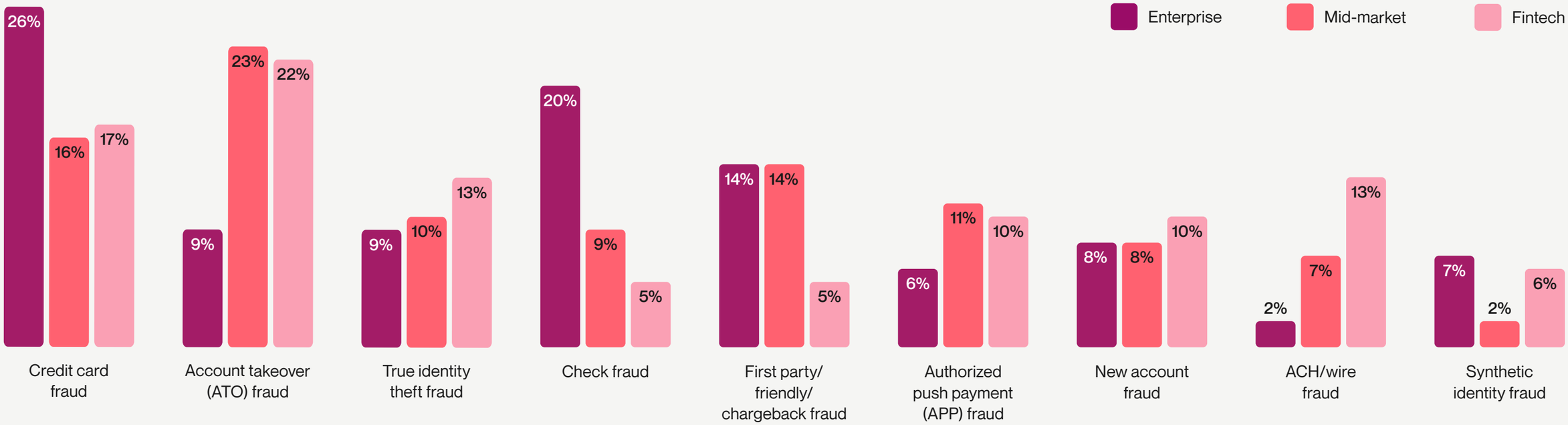
The leading fraud types reported were credit card fraud, account takeover (ATO) fraud, identity theft, and check fraud.

What type of fraud events did you see most frequently by case volume in the last twelve months?



Enterprise banks reported more credit card and check fraud than any other sector.

What type of fraud events did you see most frequently by case volume in the last twelve months?



Insight from

Q2

Jeff Scott

Vice President –
Fraudtech Solutions at **Q2**

"As fraud evolves, financial institutions are facing an ever-growing challenge to protect their customers and assets. The prevalence of ATO across sectors indicates that fraudsters are not only targeting digital channels but are also testing the resilience of legacy processes and systems. This dual pressure impacts both customer trust and institutional preparedness like never before.

To keep pace with these challenges in 2025, financial institutions must adopt a data-driven, proactive strategy — leveraging advanced fraud prevention tools like AI-driven analytics, adaptive risk scoring, and real-time interdiction — to stay ahead of bad actors."

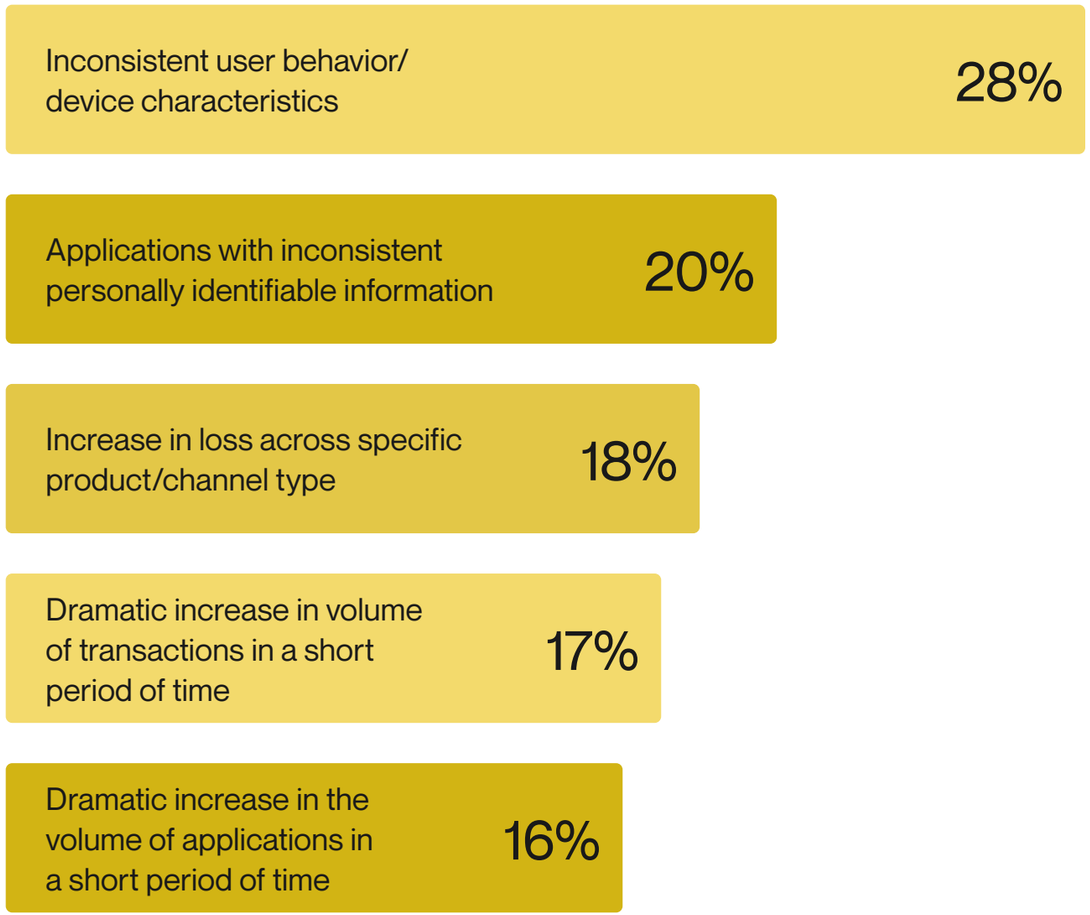
Behavior and identity inconsistencies were the leading signs of attempted fraud.

Alloy insight

Last year, we predicted the industry would see a rise in ATO attacks as fraudsters equipped themselves with increasingly sophisticated technology.

While this pattern has been proven, fraud still varies across sectors, with different types of organizations facing distinct challenges. Enterprise banks, for instance, report significantly less ATO fraud than their mid-market and fintech counterparts — likely due to their more robust fraud prevention solutions, which help prevent account takeovers in digital banking.

What's the most common flag when attempted fraud events occur?



Note: In 2024, "high velocity of transactions" was ranked as the leading sign of attempted fraud. We adjusted the wording of this option for this year's survey and also included a new category for increase in volume of applications.

Insight from

Dennis Gamiello

EVP, Global Head of Identity
at **Mastercard**

"Bad actors continue to attempt to disrupt our every day, causing reputational and monetary damage to financial institutions. As their methods of committing fraud continue to adapt, it's imperative that financial institutions of all sizes continue to leverage identity solutions as an essential component in their fraud strategies in the years ahead – so that they have effective identity verification in place, establishing trust from the onset at new customer onboarding and maintaining that trust with continuous monitoring throughout the customer lifecycle."

At 56%, most financial organizations detected fraud in real-time at the point of the transaction.

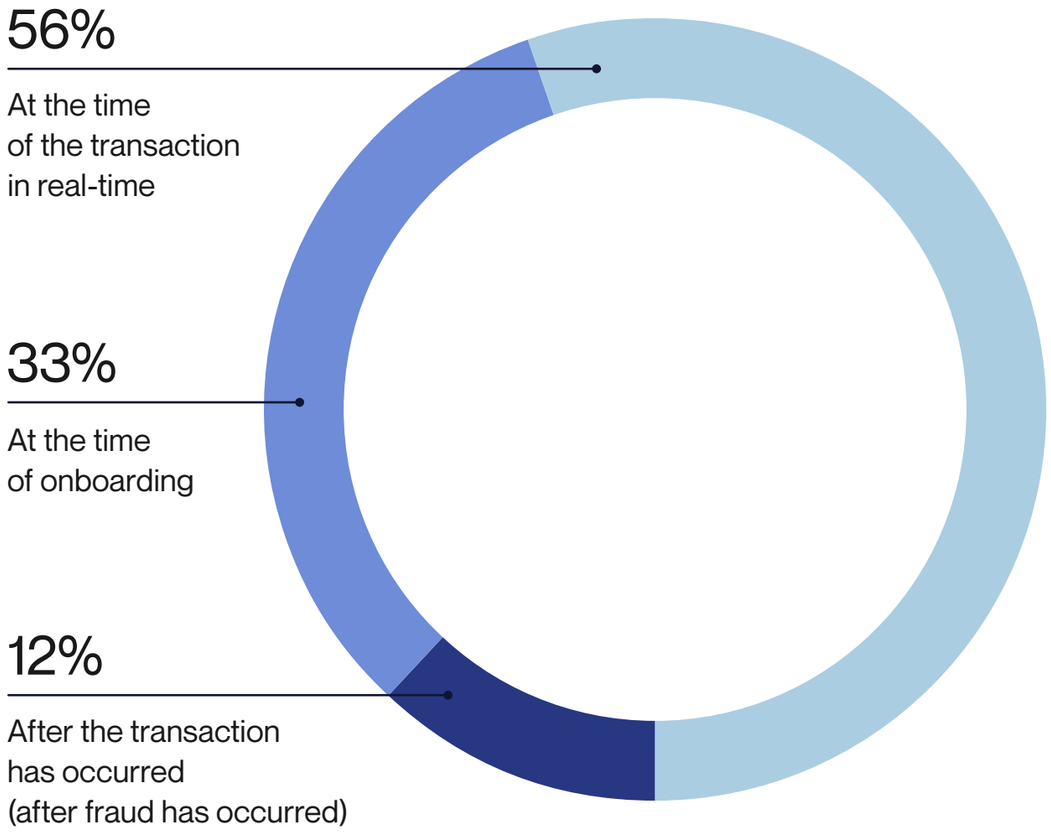
Only a third of respondents most commonly detected fraud at onboarding.

Alloy insight

Last year, 50% of respondents reported that they most commonly detected fraud at the time of the transaction, compared to 56% this year. The percentage of organizations catching fraud at onboarding has remained steady year-to-year at 33%.

The difference lies in the percentage of financial organizations detecting fraud after it has occurred, which last year stood at 17%. This suggests that organizations' investments in fraud prevention in 2024 are starting to pay off, and that there are still gains to be made in identity risk decisioning at the time of onboarding.

At what part of the customer lifecycle do you most commonly detect fraud events?



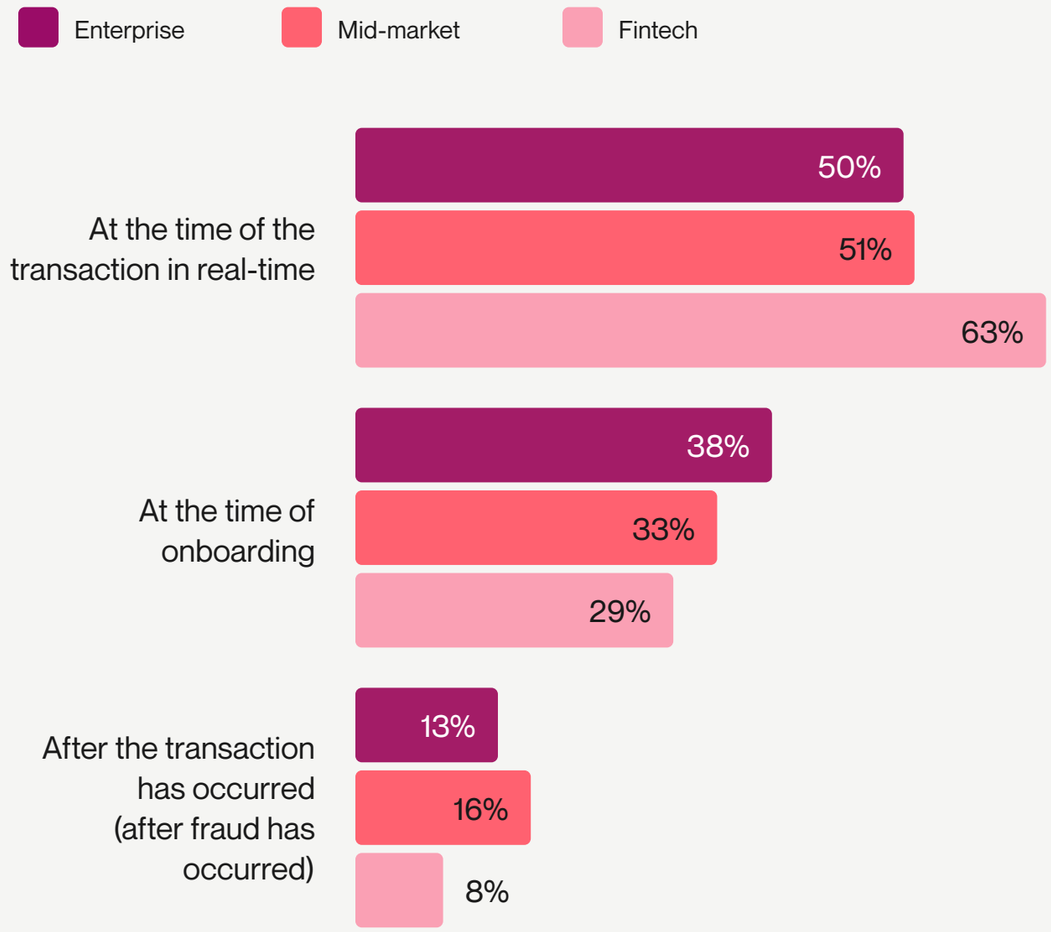
Note: This year, we added an "Other" response option to this question, which may account for variations in the reported methods YoY.

At 38%, enterprise banks led the charge to catch more fraud at onboarding.

Alloy insight

Financial organizations that identify bad actors at onboarding are more likely to prevent fraud from happening because they are able to keep bad actors out of their systems entirely. Enterprise banks detect more fraud at onboarding than any other group, indicating an investment in identity risk processes and technologies.

At what part of the customer lifecycle do you most commonly detect fraud events?



Alloy insight

While these results highlight opportunities for financial organizations to invest in fraud detection, they also reveal critical gaps in how fraud is managed after detection.

Detecting fraud in real-time doesn't necessarily mean action is taken immediately. Many organizations detect fraud but do not pause or interdict the transaction at that time, opting instead to triage the event through manual intervention. This approach can lead to transactions being successfully processed even when fraud is suspected, putting the organization in a challenging position once the fraud is confirmed.

The lag between detection and triaging is a key vulnerability. Some financial institutions and fintechs may not get around to addressing fraud for days — likely either due to a staffing issue or inefficient systems, allowing funds to be stolen despite the presence of real-time fraud detection capabilities. Addressing this gap is essential for strengthening fraud prevention strategies.

Often, financial institutions do not interdict in real-time because the only tool they have is to block the transaction while waiting for a review, which hinders customer experience. Instead, financial institutions and fintechs should leverage active step-up verification — such as ID/selfie or device-based verification — for riskier transactions. Ultimately, step-up verification enables FIs to stop the riskiest transactions without blocking the flow of funds for customers who are able to self-resolve.

Fraud costs and consequences

Nearly 1 in 3 financial organizations experienced direct fraud losses surpassing $1M.

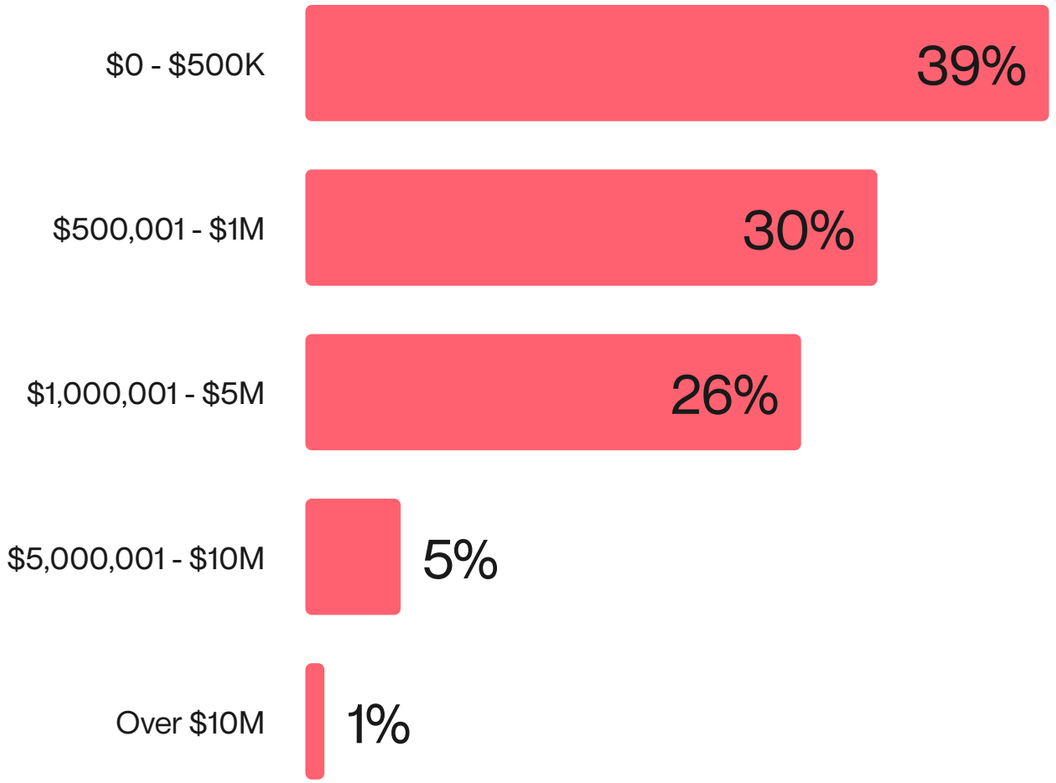
31% of financial organizations incurred over **$1M** in direct fraud losses.

61% of financial organizations incurred over **$500K** in direct fraud losses.

Alloy insight

This is higher than the metric we recorded in 2024, when 1 in 4 respondents reported losses surpassing $1M. The impact of fraud is even more staggering when you consider that direct loss doesn't include expenses such as regulatory fines and money spent recouping funds.

How much money has your organization incurred in **direct fraud losses** in the last twelve months?



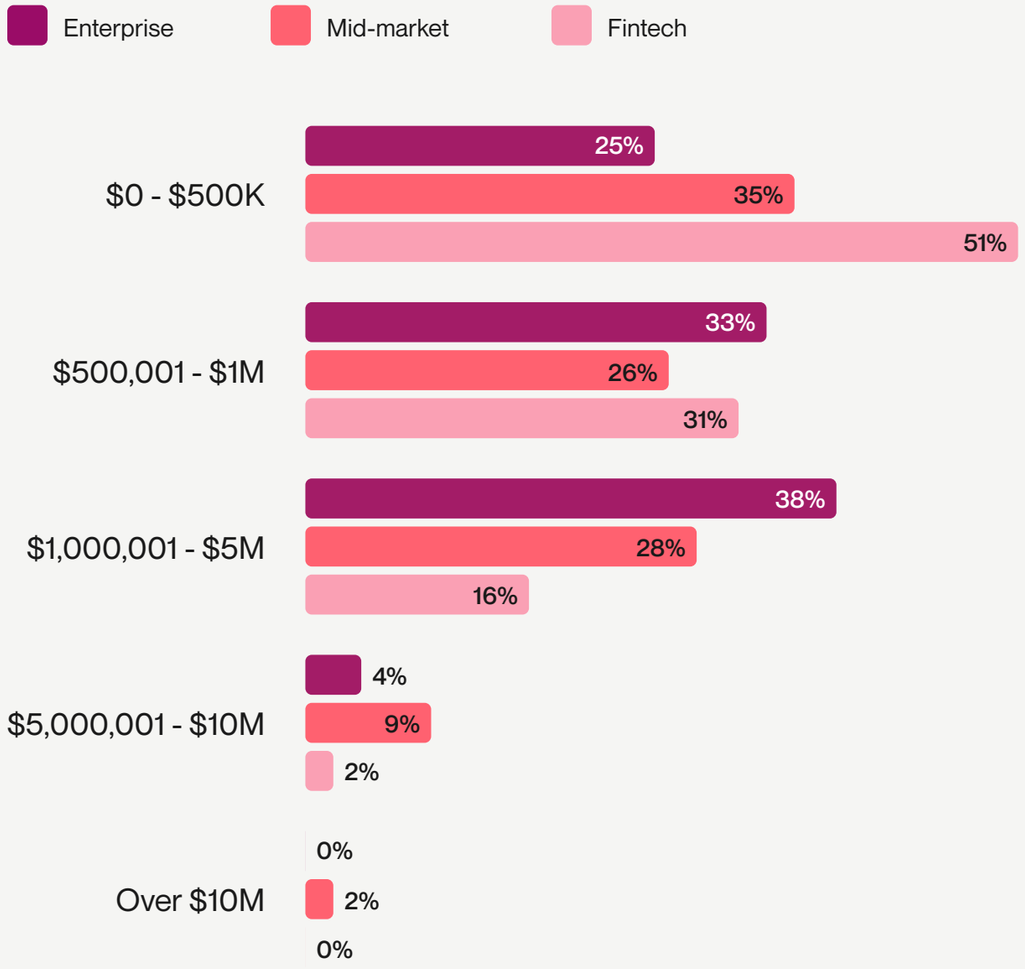
11% of mid-market banks and credit unions reported over $5M in direct fraud losses last year.

Mid-market banks and credit unions reported the highest percentage of $5-10M losses. Mid-market was also the only sector to report losses over $10M.

42% of enterprise banks incurred over **$1M** in direct fraud losses.

75% of enterprise banks incurred over **$500K** in direct fraud losses.

How much has your organization incurred in **direct fraud losses** in the last twelve months?



Despite steep direct financial losses, reputational damage was ranked as the most impactful consequence of fraud.

On average, financial organizations consider the most consequential negative effects of fraud to be reputational damage, direct financial losses, and loss of clients.

Top Fraud Consequences Negatively Impacting Financial Organizations

1	Reputational damage	73%
2	Direct financial losses	72%
3	Loss of clients	72%
4	Loss due to goodwill credit to client	70%
5	Regulatory fines/penalties	70%
6	Legal repercussions	67%

Fraud preparedness and prevention

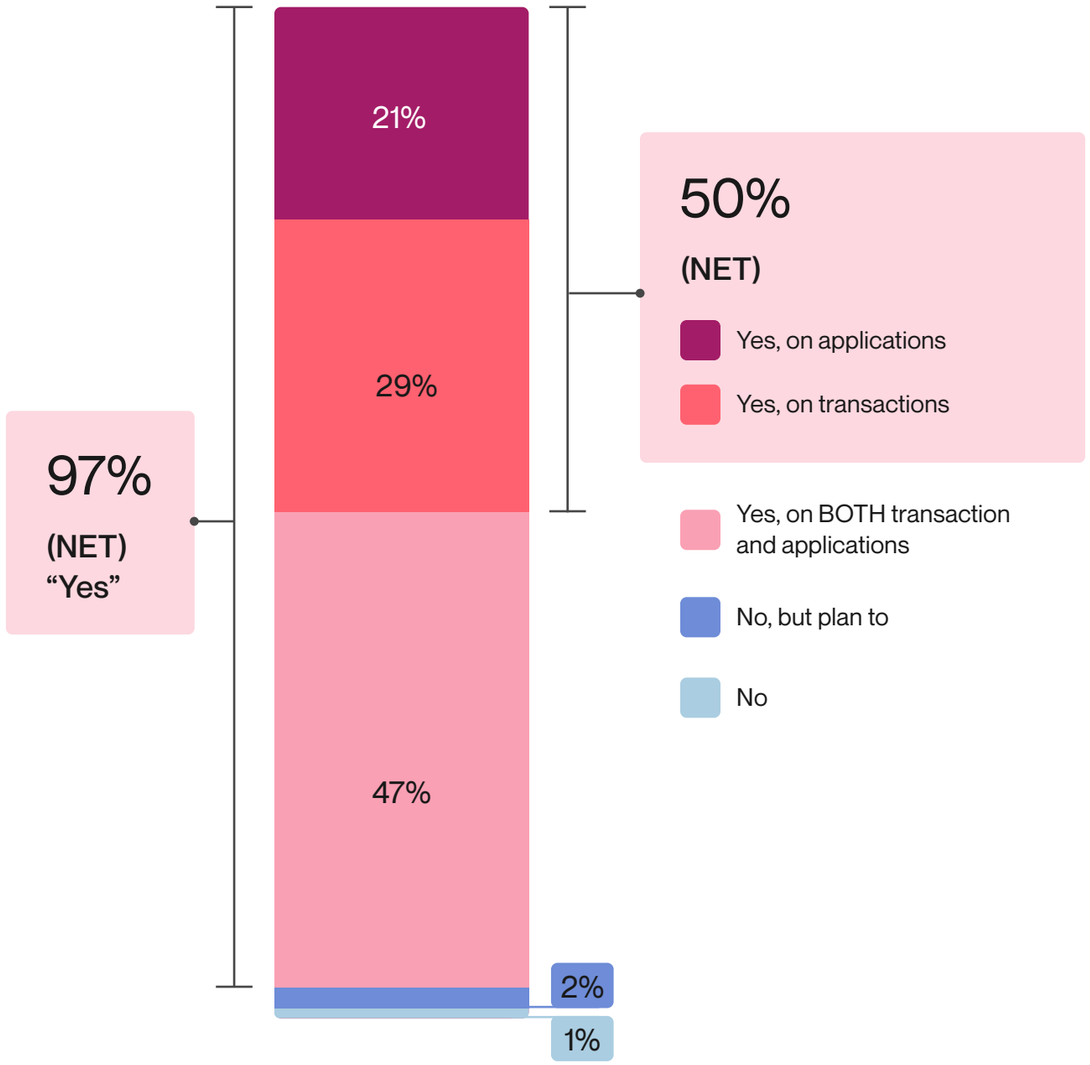
Survey results reveal a significant gap in real-time fraud protection.

At 47%, less than half of financial organizations conducted real-time interdiction on both applications and transactions; 50% of respondents said they only did so on one or the other.

Alloy insight

Without comprehensive real-time monitoring, financial institutions may not detect fraud for days after an attack, miss opportunities for customers to self-resolve suspicious activities, and face increased back-office burden from manual investigations. They also risk unnecessary exposure to fraudulent monetary movement that could have been prevented. This protection gap is particularly concerning, as fraudsters often exploit weaknesses in either the application or transaction stage — making it crucial to monitor both points in real-time.

Does your firm conduct real-time interdiction?



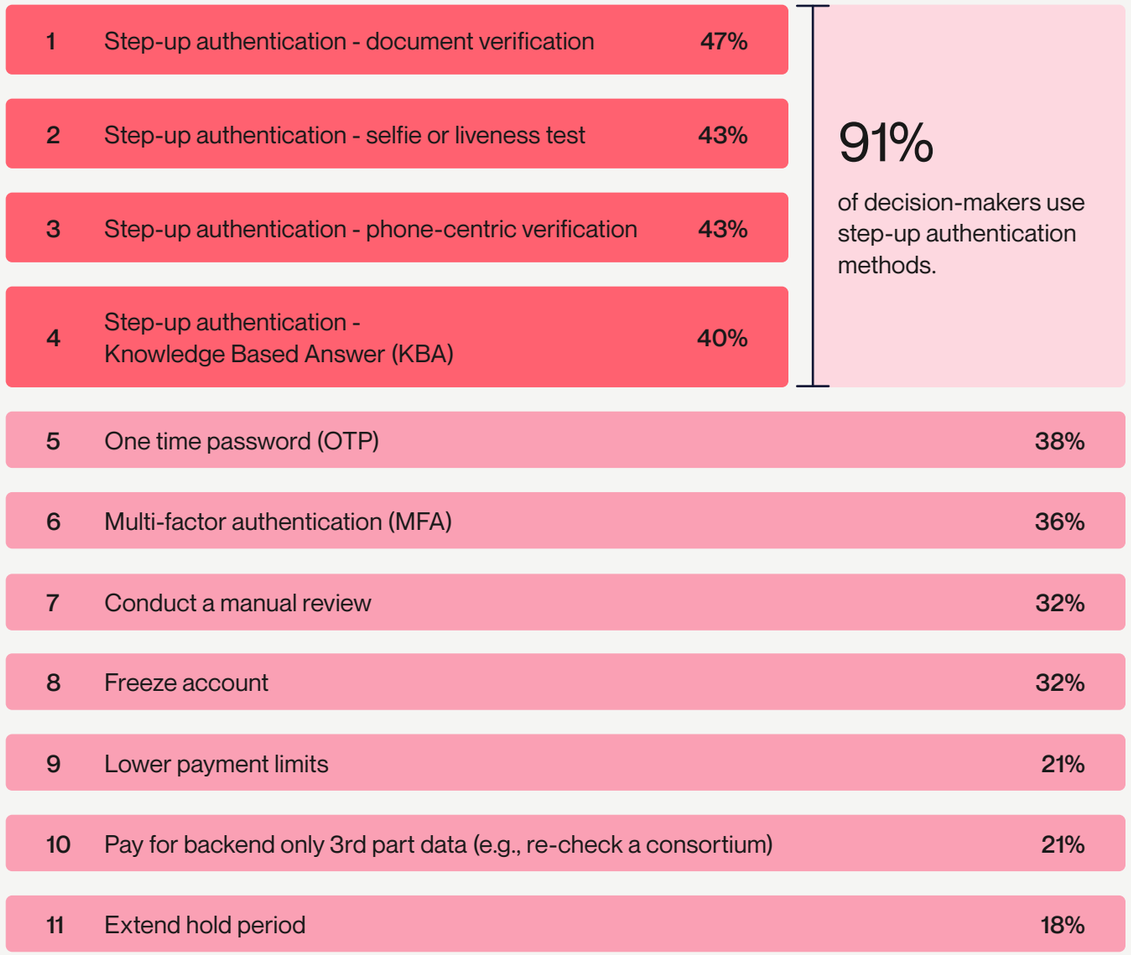
91% of financial organizations reported step-up authentication as a first response once fraud is detected.

Alloy insight

KBA usage continues to decline, with 40% of respondents using it as a verification step — down from 47% last year.

Though many organizations still rely on KBA, this decrease reflects a broader industry shift toward more secure and user-friendly verification methods like document verification and biometric authentication.

Once an anomaly or risk is identified, what do you do about it? (Select all that apply.)



Note: This year, we added four new response options to this question (OTP, MFA, manual review, and pay for backend), which may account for variations in the reported methods.

Insight from

UBT
Union Bank & Trust®

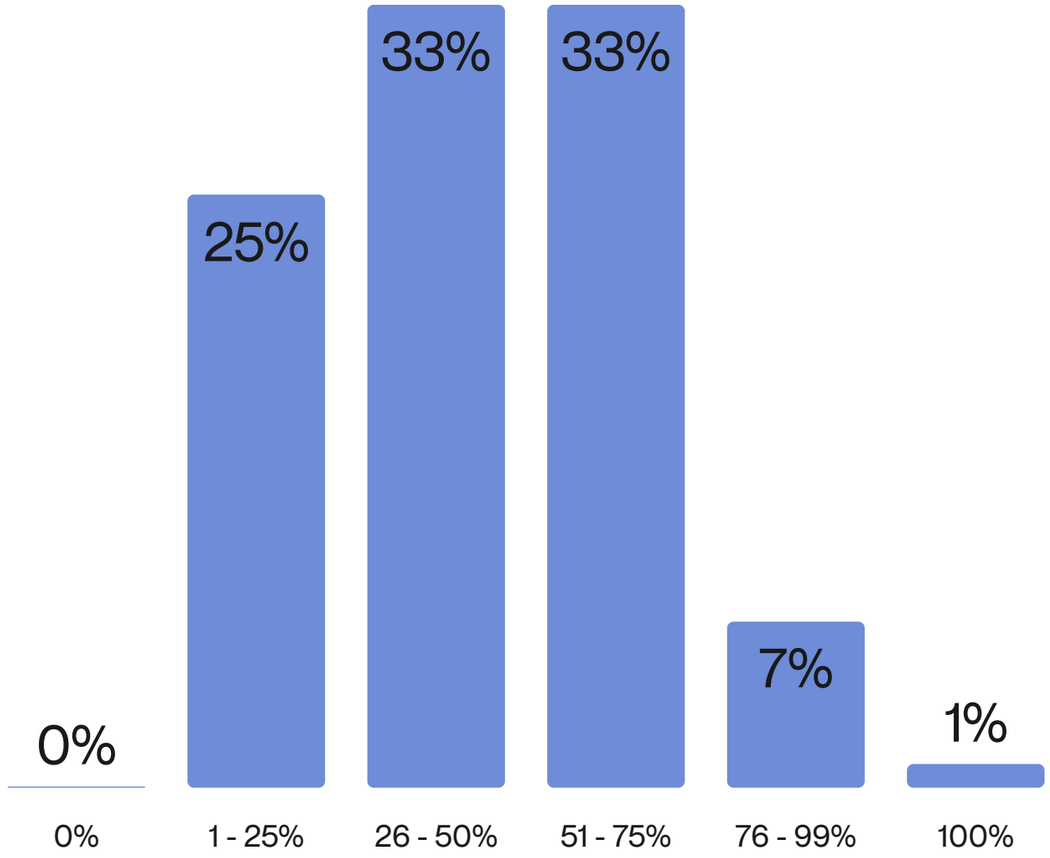
Jon VanMeter

Vice president, Bank Secrecy Act Officer
at **Union Bank & Trust Company**

"Step-up authentication tools, including documentation verification with selfie and liveness tests, helped us enhance customer identification and boost efficiency. By adopting these step-up authentication methods, we reduced manual reviews by nearly 85%, allowing our staff to focus on serving our customers."

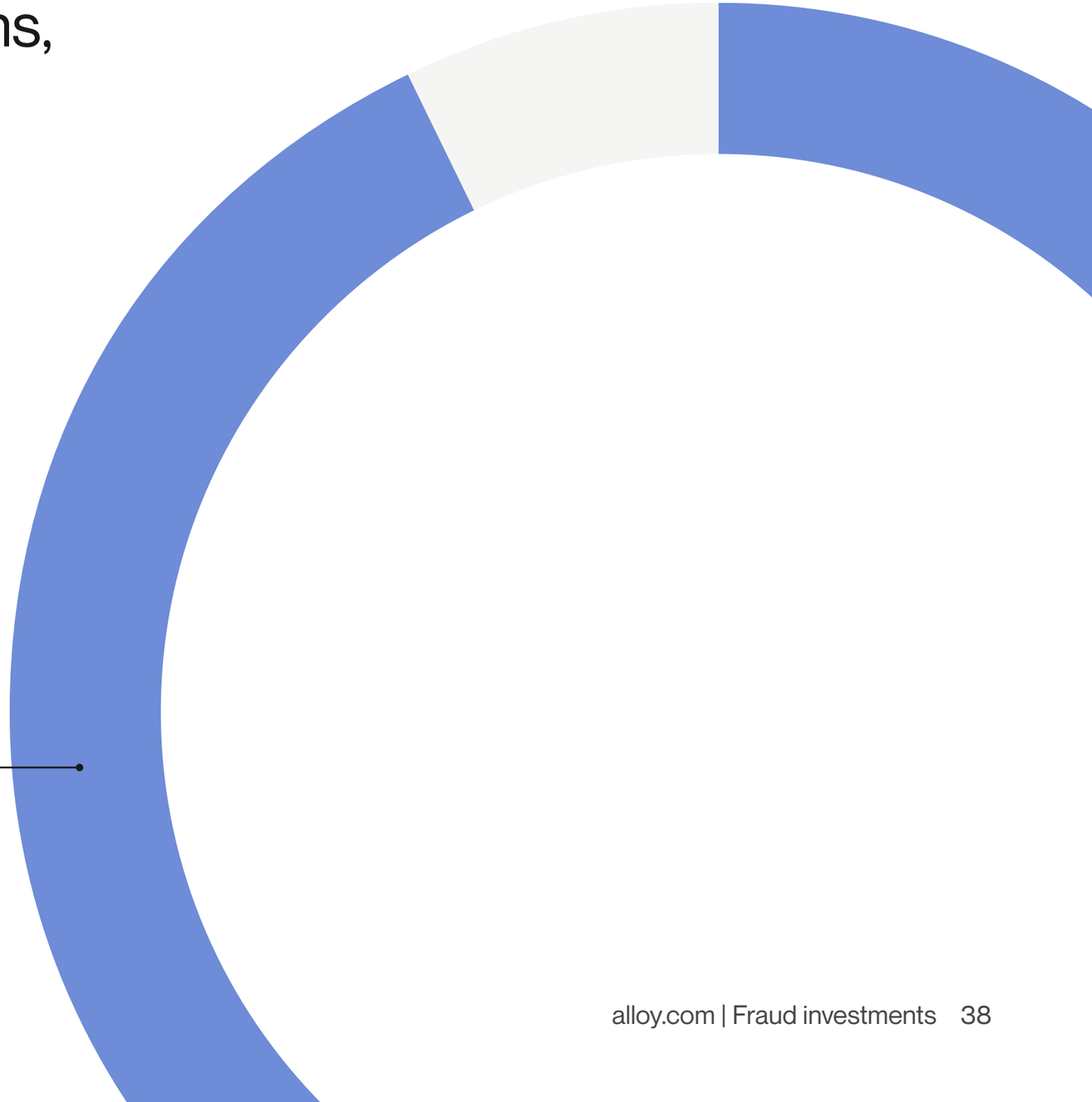
3 in 4 financial organizations reported that more than 25% of new account applications required manual review.

What percentage of new account applications require a manual fraud review by your analysts?



Fraud investments

With rising fraud and tighter regulations, financial institutions and fintechs are stepping up their defenses.

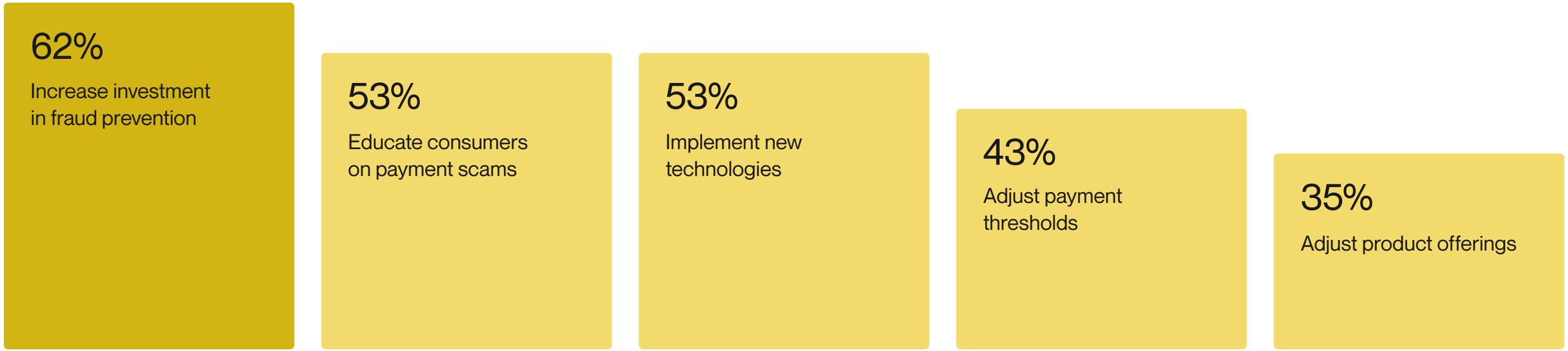


93%

of respondents said that their organization is **making ongoing investments** in fraud prevention in 2025.

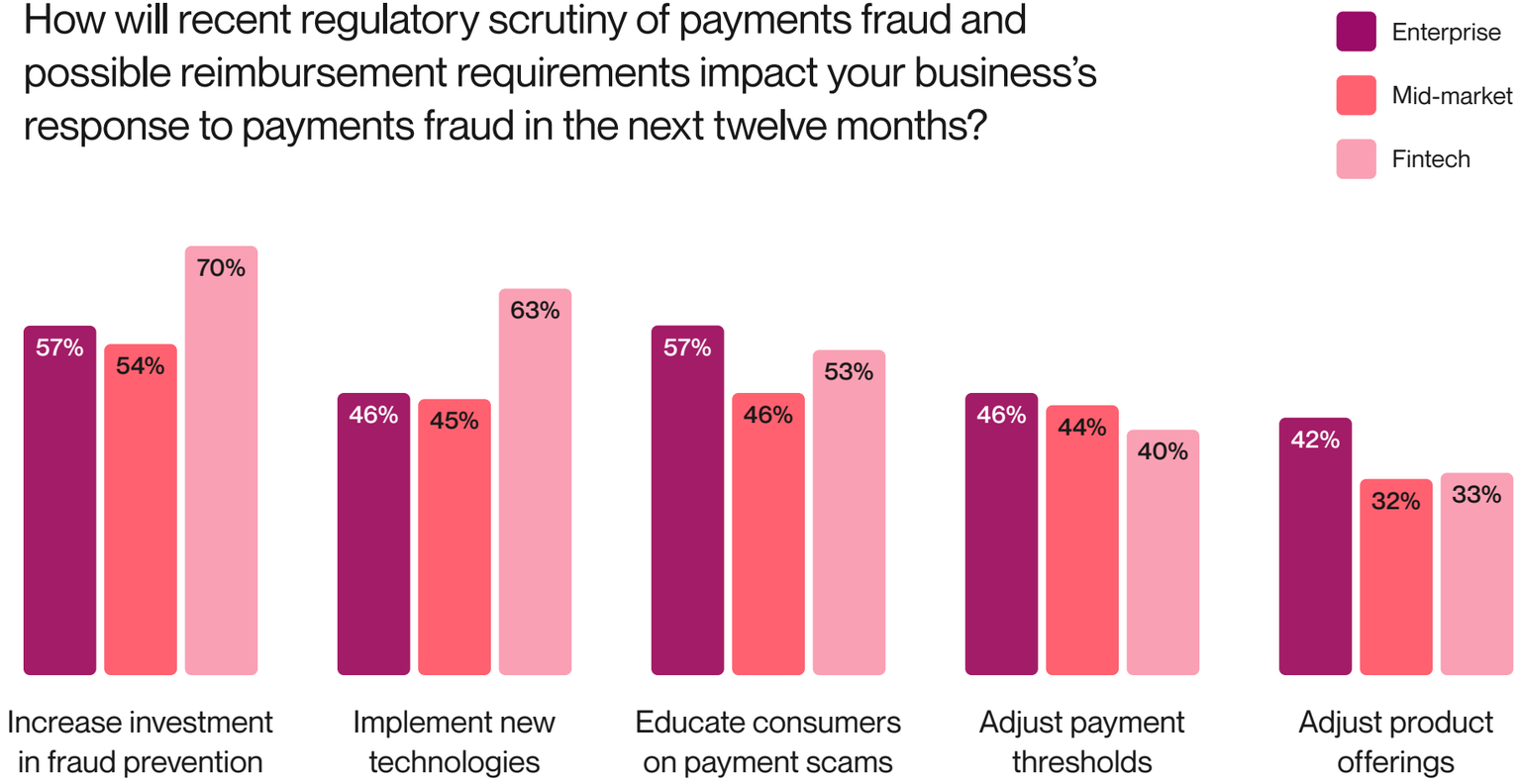
Nearly two-thirds of financial organizations reported plans to invest more in fraud prevention in response to recent regulatory scrutiny.

How will recent regulatory scrutiny of payments fraud and possible reimbursement requirements impact your business's response to payments fraud in the next twelve months?



Increasing investment in fraud prevention is the leading response to recent regulatory scrutiny.

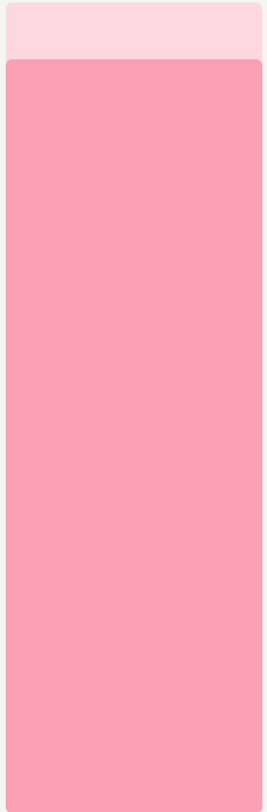
How will recent regulatory scrutiny of payments fraud and possible reimbursement requirements impact your business's response to payments fraud in the next twelve months?



Alloy insight

At 57%, enterprise banks say educating consumers on payment scams is just as important as increasing investment in fraud prevention. While only 15% of respondents said that customer coercion is the leading cause of fraud attempts, sophisticated scams often blend technical exploitation with social engineering, supporting the need for both enhanced security measures and customer awareness.

99% of respondents report using AI as a part of their fraud prevention system.



93%

agreed that machine learning and generative AI will **revolutionize fraud detection.**

How are you using machine learning and/or AI as part of your fraud prevention system?

99%
(NET) Use AI

- **67%** — Providing explainability for large data sets, such as providing reasons for why transactions were rejected, or creating narratives for SAR reporting
- **59%** — Supplementing rule-based decisioning with supervised machine learning models (in-house and third party) to detect anomalous activity
- **59%** — Automating operations / investigations, such as minimizing manual tasks to save time and resources
- **1%** — We do not use machine learning and/or generative AI as part of our fraud prevention system

Insight from

SentiLink

"While GenAI introduces novel attack vectors and accelerates some old ones, it's also a tool that can be used for good. For example, large language models (LLMs) can ingest customer communications and may be able to detect victims being scammed, or process transaction logs and identify unauthorized transactions or money laundering. So over the next few years we predict both AI-enabled fraud attacks as well as novel controls that this new technology makes possible.

The two things that AI can't fake are history and authority. GenAI can deepfake a person's face and voice, but it can't create an email address for them that already has ten years of history. And GenAI can make up a fake SSN, but it can't get the SSA to say that it passes eCBSV. In order to "AI-proof" their fraud controls, it's crucial that financial institutions rely on tools that have a deep understanding of fraud and identity."

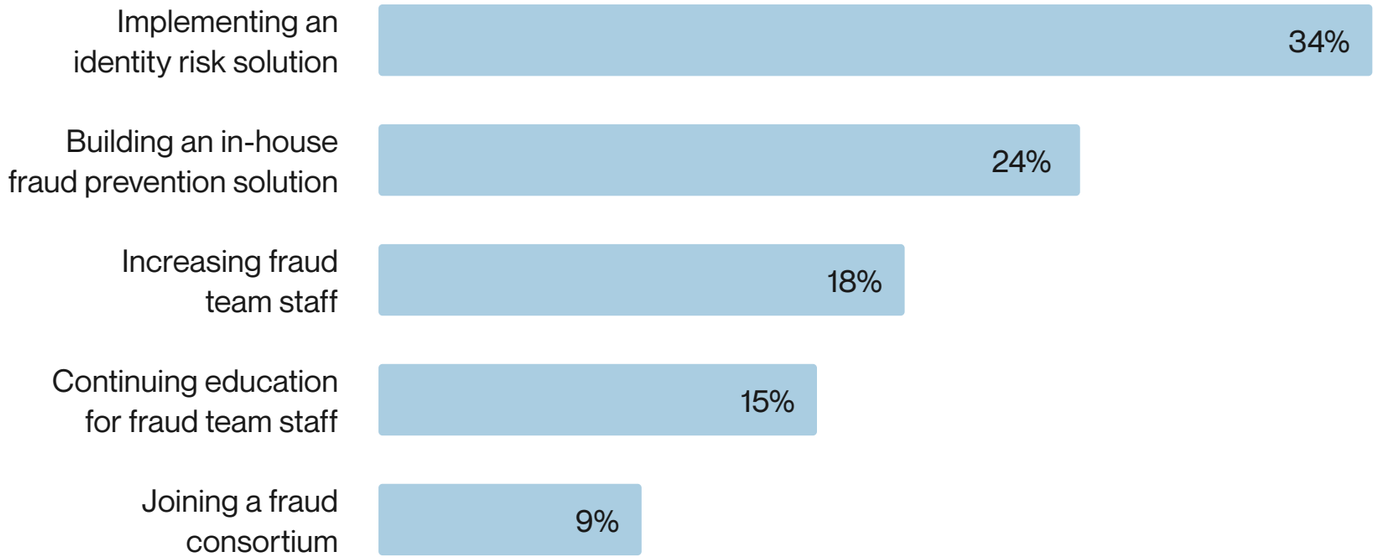
Naftali Harris

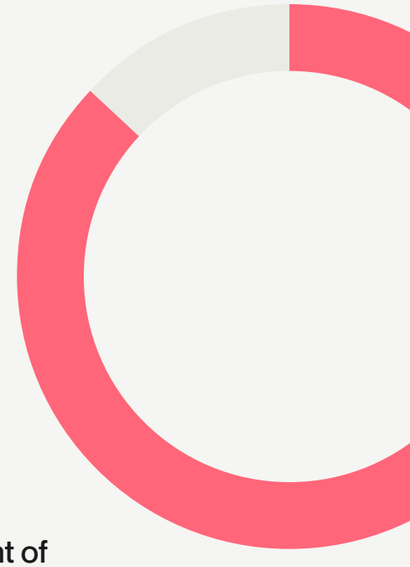
Co-founder and CEO at **Sentilink**

Investments in fraud prevention are paying off.

Over 1 in 3 decision-makers said that investing in an identity risk solution had the biggest impact on reducing fraud rates.

What investment has had the greatest impact on reducing fraud rates at your organization over the course of the last twelve months?





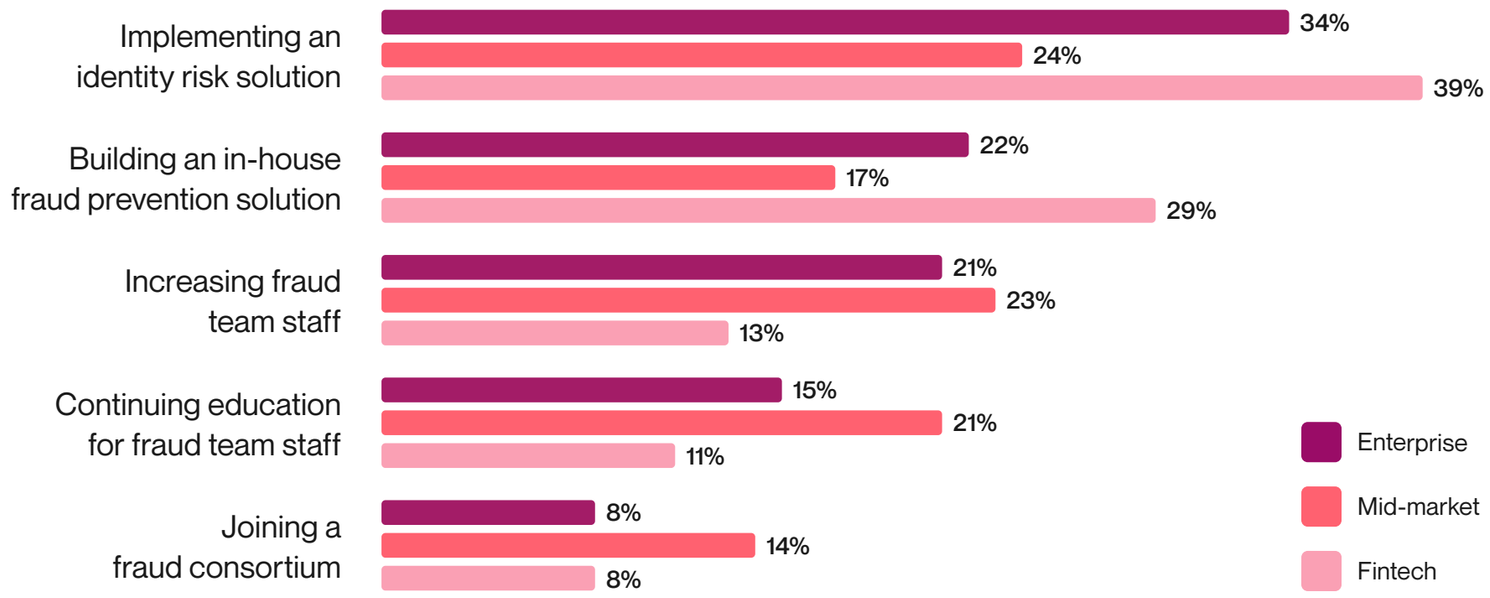
87%

agreed that the amount of money saved by fraud prevention investment outweighs its cost.

Enterprise: 92%
Mid-market: 83%
Fintech: 86%

Identity risk solutions were popular across sectors, especially among fintechs and enterprise banks.

What investment has had the greatest impact on reducing fraud rates at your organization over the course of the last twelve months?



Alloy insight

Mid-market banks and credit unions prioritized increasing fraud staff and ongoing education, placing these investments neck-and-neck with identity risk solutions.

This reliance on internal resources and staff development reflects a more traditional approach to fraud prevention, despite the consensus that money spent on fraud prevention technology is worth the benefits.

In contrast, fintechs focused almost exclusively on technology, aligning their strategies with the broad consensus that implementing an identity risk solution is the most impactful investment for reducing fraud.

Finally, enterprise banks were able to strike a balance, with 56% reporting investments in either building an in-house fraud prevention solution or purchasing an identity risk solution. This blended approach combines technological measures with operational enhancements like increasing headcount.

64% of organizations reported plans to invest in identity risk solutions in 2025.

What types of technologies will you be looking to invest in the next twelve months?

1	Identity risk solution	64%
2	Document verification software	49%
3	Anti-scam education tools	38%
4	Voice, facial, and fingerprint recognition	38%
5	Machine learning	35%
6	Alternative data vendors	33%

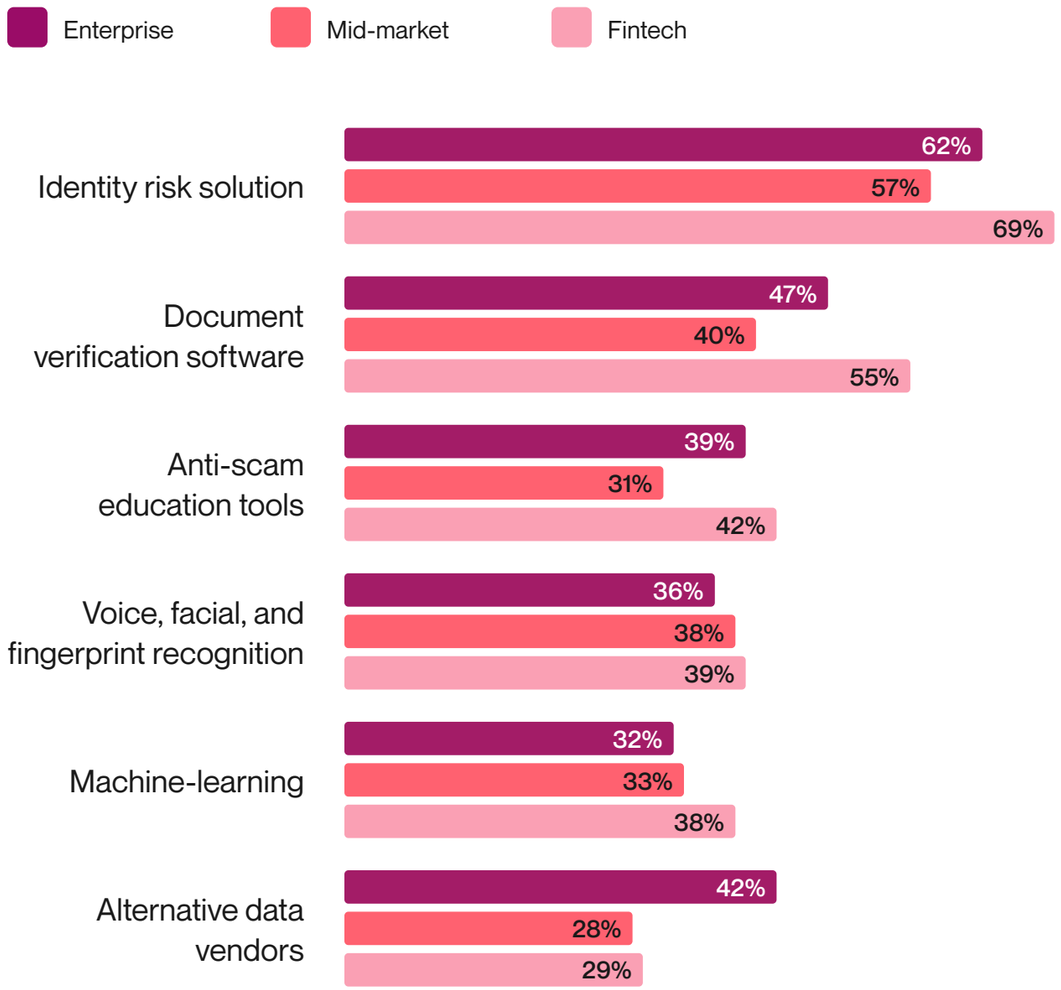
Enterprise banks expressed a stronger interest in alternative data investments.

Alloy insight

Financial organizations have traditionally relied on conventional data sources, such as credit bureau data. However, now, enterprise banks are recognizing the importance of integrating alternative data sources (such as cash flow analytics) into their fraud prevention strategies.

Too often, data critical to accurate customer decisioning is inaccessible or siloed within enterprise banking systems. Data orchestration can help these large financial organizations pull information from multiple data sources, including alternative ones. This process streamlines fraud management workflows into a single configuration, resulting in more efficient, effective, and compliant fraud prevention.

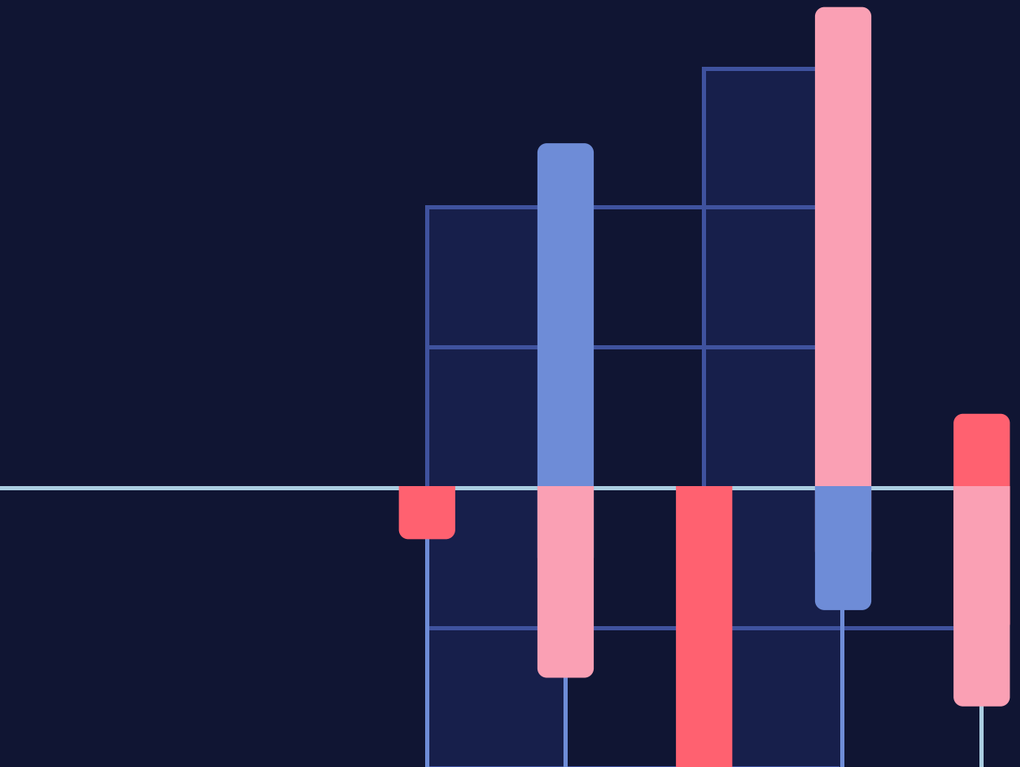
What types of technologies will you be looking to invest in the next twelve months?



Fraud predictions

Where will fraud go next in 2025?

A prediction from **Tommy Nicholas**
CEO of Alloy



On AI as a fraud prevention tool

Fraud will continue its upward trajectory in 2025, fueled by the sheer volume of consumer personal information available on the dark web. Data breaches at major telecom and health insurance companies have created a treasure trove of sensitive data, making it easier for fraudsters to orchestrate sophisticated attacks.

While headlines may focus on AI as both a tool for fraudsters and a solution for financial institutions, the reality will be more grounded: this year will see fewer overhyped promises about AI and more tangible applications of machine learning to address fraud in real-time.

Rather than relying on standalone AI tools, financial organizations will shift their focus to investing in platforms that centralize identity and fraud risk across their organizations. These holistic solutions will enable financial organizations to unify point solutions, providing a clearer, more comprehensive view of risk. This trend began gaining momentum in 2024 but is poised to take off in 2025 as financial institutions and fintechs recognize the dual benefits: reducing fraud rates and improving operational efficiency.

Expect the conversation around fraud prevention to move beyond buzzwords as institutions adopt practical, integrated strategies that align technology with broader organizational goals. Machine learning will remain a critical tool, but the real shift will come from how financial institutions reimagine their systems to stay ahead of evolving threats.

Where will fraud go next in 2025?

A prediction from **Parilee Wang**
Chief Product Officer

On key fraud drivers

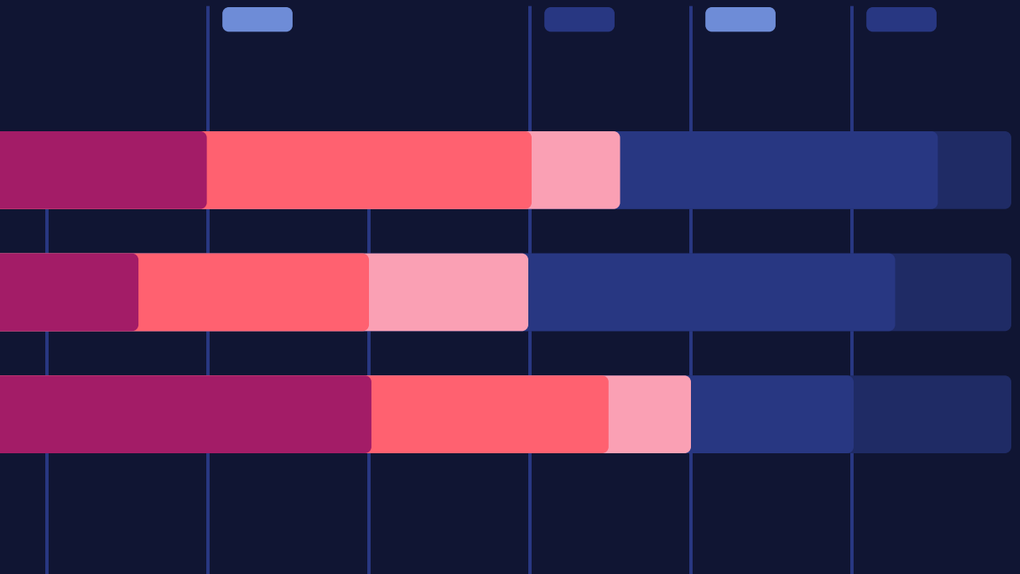
AI will continue to be a key fraud driver in 2025, especially as bad actors use it to become more efficient at targeting financial institutions and their customers. Technologies like deepfakes and voice cloning will make it harder for consumers to detect these scams, especially in the case of senior citizens and other vulnerable populations.

With money movement happening more quickly in the digital world, it will become increasingly important for banks to get a lid on account takeover (ATO) fraud, which occurs when a customer's credentials are stolen, and may result in money leaving their account without their knowledge.

Preventing ATO fraud will require a shift in strategy for financial institutions. They'll need to stop relying as heavily on transaction monitoring and focus on identity. This will allow them to assess risk before customers begin transacting by leveraging fraud indicators that show up much earlier. Many FIs are already leveraging AI and ML products to detect these early trends to positive results.

Where will fraud go next in 2025?

A prediction from **Sara Seguin**
Principal Advisor of Fraud & Identity Risk



On real-time and peer-to-peer payments

In 2025, banks will double down on implementing tools to better prevent fraud that occurs via peer-to-peer (P2P) payments platforms as well as payments rails like RTP and FedNow.

Financial institutions that improve their fraud prevention processes before regulators force their hand will be best positioned to profit off of their payments businesses. Expect US policymakers to continue the regulatory scrutiny of payments fraud after watching regulators in Australia and the UK take similar action. With a new administration underway, this is unlikely to accelerate in year one. However, I suspect it will be an ongoing focus.

Next year, we will see an increase in real-time payments fraud driven by the rise of AI tools being utilized by fraudsters. Consumers will be subject to increasingly convincing scams on social networks that are designed to encourage them to move money quickly, regardless of their instincts.

To better prevent real-time payments fraud, banks will need to take a multi-layered approach that prioritizes stopping fraud at onboarding, using real-time interdiction when risk is suspected, and incorporating multiple signals in advance of the money movement, such as behavioral biometrics and device risk.

While it can be difficult for banks to move quickly due to their highly regulated nature, I am optimistic that we will see banks make strides towards stopping payment fraud through an omnichannel approach in 2025.

Conclusion

Conclusion

In last year's State of Fraud Report, a quarter of respondents named AI fraud their most pressing concern for the coming year.

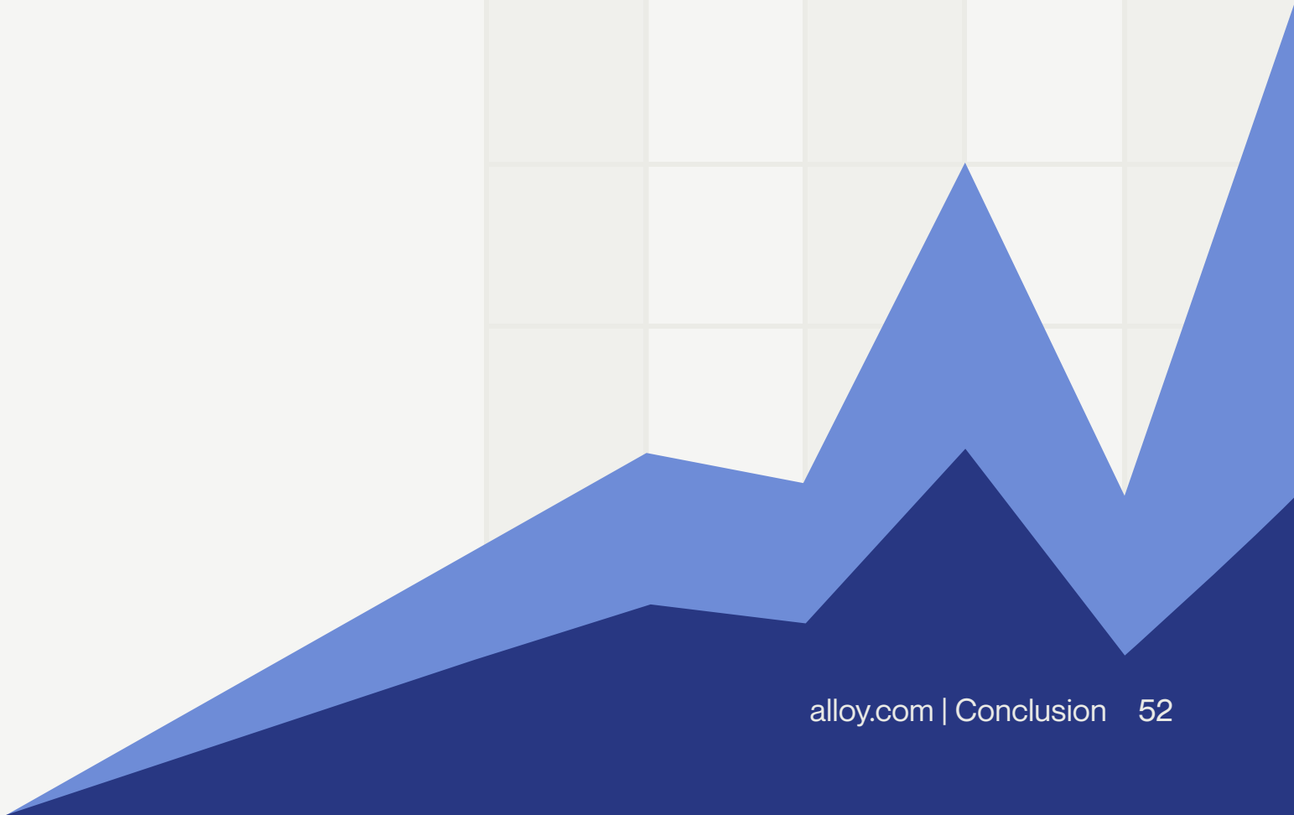
2025 marks a significant shift from theoretical AI applications to practical implementations, both by fraudsters and financial organizations. AI has a 99% adoption rate among decision-makers surveyed.

Meanwhile, professional fraudsters are taking advantage of consumer information exposed by AI-assisted scams and data breaches. Financial organizations are taking note, with 71% of respondents agreeing that financial criminals and crime rings are responsible for most of the fraud at their organization.

While AI is driving the commercialization of fraud by pushing costs down for bad actors and enabling efficient, scalable processes, the cost of fraud has gone up for financial organizations. One in three report losing more than a million dollars due to fraud in the past year — up from one in four the year prior.

Still, organizations are optimistic. AI-powered fraud prevention models can alert organizations to fraud attacks in real-time so they can contain those activities and act on risk.

The best way to stop fraud from happening is to drive fraudsters out of business. Moving forward, greater fraud prevention investments will continue to raise the cost of committing fraud for bad actors, potentially evening out the advantage gained from tools like FraudGPT and the dark web.



Segment snapshots

Enterprise bank snapshot

Frequency of fraud events YoY	Consumer accounts	Business accounts
(NET) Increase	66%	67%

Total fraud events in the past year	Consumer accounts	Business accounts
(NET) 1,000+ Cases	46%	47%

Direct fraud losses	
> $500K - 1M	33%
> $1M - 5M	38%
$5M+	4%

Top digital channel control
52% Two-factor authentication

Top physical channel control
56% Document verification

Top fraud channel
59% Online banking

Top fraud type
26% Credit card fraud

Top fraud consequences		
80% Financial loss	76% Goodwill loss	76% Damaged reputation

Top investment for 2025
62% Identity risk solution

Mid-market banks & credit unions snapshot

Frequency of fraud events YoY	Consumer accounts	Business accounts
(NET) Increase	52%	53%

Total fraud events in the past year	Consumer accounts	Business accounts
(NET) 1,000+ Cases	55%	57%

Direct fraud losses	
> $500K - 1M	26%
> $1M - 5M	28%
$5M+	11%

Top digital channel control
46% Two-factor authentication

Top physical channel control
59% Two-factor authentication

Top fraud channel
56% Online banking

Top fraud type
23% ATO & Identity theft

Top fraud consequences		
69% Goodwill loss	67% Client attrition	67% Financial loss

Top investment for 2025
57% Identity risk solution

Fintech snapshot

Frequency of fraud events YoY	Consumer accounts	Business accounts
(NET) Increase	60%	57%

Total fraud events in the past year	Consumer accounts	Business accounts
(NET) 1,000+ Cases	38%	33%

Direct fraud losses	
> $500K - 1M	31%
> $1M - 5M	16%
$5M+	2%

Top digital channel control
64% Two-factor authentication

Top physical channel control
64% Document verification

Top fraud channel
65% Online banking

Top fraud type
22% ATO fraud

Top fraud consequences		
74% Damaged reputation	74% Client attrition	71% Fine/penalties

Top investment for 2025
69% Identity risk solution

About Alloy

Alloy provides an Identity and Fraud Prevention Platform that enables global financial institutions and fintechs to manage identity risk so they can grow with confidence. Over 600 of the world's largest financial institutions and fintechs turn to Alloy's end-to-end platform to access actionable intelligence and the broadest network of data sources across the industry, as well as stay ahead of fraud, credit, and compliance risks. Founded in 2015, Alloy is powering the delivery of great financial products to more customers around the world.

Learn more at alloy.com