



2024

# State of Fraud Benchmark Report

Fraud trends and predictions

# How did fraud affect US financial institutions in 2023?

54%

of respondents experienced more than \$500K in direct fraud losses.

57%

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

50%

reported catching fraud most commonly in real-time.

35%

experienced 1,000+ fraud attempts—roughly 1 in 10 respondents experienced over 10,000.

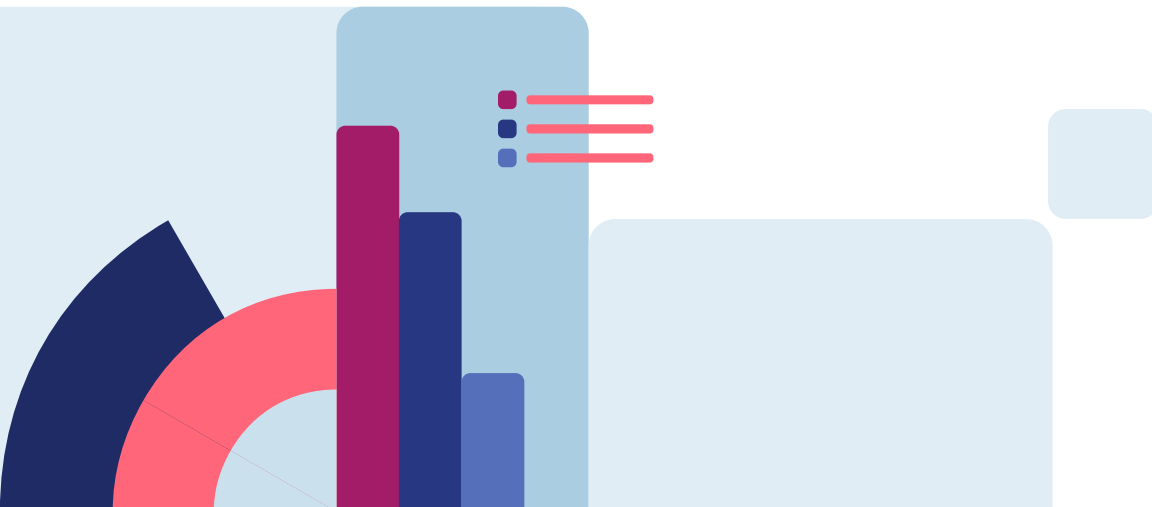
Alloy surveyed a total of 450 decision-makers — 250 in the US and 200 in the UK — working in fraud-related roles at financial institutions ranging from startup fintech companies to enterprise banks. This report gauges how both fraud and fraud prevention have changed over the last 12 months.

In 2023, fraud continued to be a significant issue for banks, fintechs, and credit unions in the US and UK. Even though organizations reported a slight decrease in the instances of successful fraud compared to the previous year's data, the majority are still seeing an increase in fraud attempts.

According to respondents, financial institutions continue to make significant investments in fraud prevention, and more of them are turning to outside sources for assistance. Meanwhile, their fraud prevention models are largely focused on transaction monitoring, as opposed to identity decisioning. However, they expressed more interest in investing in an Identity Risk Solution compared to 2022, signaling growing awareness of the importance of preventing fraud at onboarding.

# Table of contents

04	About the survey
06	Key findings in both the US and the UK
08	Fraud trends in the US
32	The cost of fraud in the US
41	Fraud predictions for 2024
48	Conclusion
50	Appendix



# About the survey

# About the survey

## Methodology

The survey was conducted from October 29 - November 17, 2023.

Respondents included 450 decision-makers working at financial services in the following sectors:

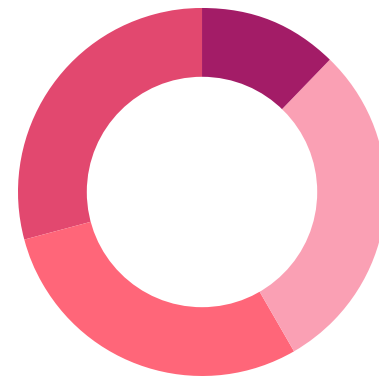
- Fintechs
- Online or Pure-Play Lending Institutions
- Enterprise Banks
- Mid-Market Banks
- Regional Banks
- Community Banks/Credit Unions

Of the 450 decision-makers:

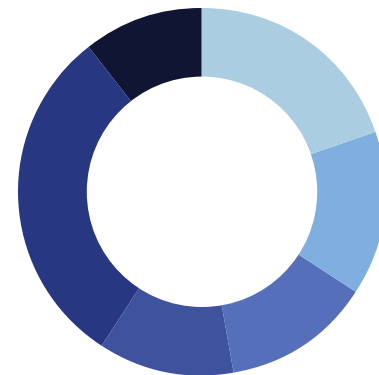
- 250 were based in the US
- 200 were based in the UK

The survey was conducted by **Qualtrics**, a leading survey platform which powers +1B surveys every year.

## Demographic segments



- Growth Fintech: *fintech + 1-100 employees* (3%)
- Strategic Fintech: *fintech + 101-250 employees* (7%)
- Mid-Market Fintech: *fintech + 500-1000 employees* (7%)
- Enterprise Fintech: *fintech + more than 1,000 employees* (7%)

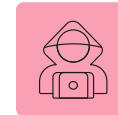


- Enterprise Bank: *national bank + bank + more than \$50B in assets* (15%)
- Mid-Market Bank: *national bank + regional bank + bank + \$10B to \$50B in assets* (11%)
- Regional Bank: *national bank + regional bank + bank + less than \$10B in assets* (10%)
- Credit Union/Community Bank (9%)
- Online/Pure-Play Lending Institution (23%)
- Other (8%)

# Key findings across both the US and the UK



Most fraud happens via internet-based platforms such as mobile and online/digital services.



Respondents see bust-out fraud and authorized push payment (APP) fraud as the most prevalent fraud types. They also report these fraud types are responsible for their organizations' greatest financial losses.

**25%**

of companies lost over 1 million EUR/USD to fraud in 2023.



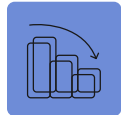
**3 of 4**

banks and fintechs are planning to invest in an Identity Risk Solution in the next 12 months to combat fraud.



# Year over year (YoY)

## What changed from 2022-2023?



Fraud is still increasing, but at a slower rate than last year.

- **98%** experienced fraud in 2023, but the number and frequency of fraud attempts occurred at a slower rate than the previous year.
- Respondents experienced fewer financial setbacks, but they also recovered fewer of these financial losses compared to 2022.



There is a shift toward outside resources for fraud prevention.

- Fewer development team members are focused on fraud-related activities, most likely due to outsourcing.
- Approximately **52%** allocate funds to third-party solutions to combat fraud, a significant uptick.

## What stayed the same?




Fraud detection techniques and responses to fraud are largely consistent.

- In 2023, fraud detection commonly occurred during real-time transaction monitoring, consistent with findings from 2022.
- Respondents cited “dramatic increases in volume of transactions over a short period of time” as the leading indicator of attempted fraud.
- Step-up authentication actions continued to be the first course of action once risk was identified.
- Organizations that implemented fraud prevention tools experienced tangible process efficiency benefits, including a higher likelihood of catching fraud at onboarding and a decrease in manual reviews.

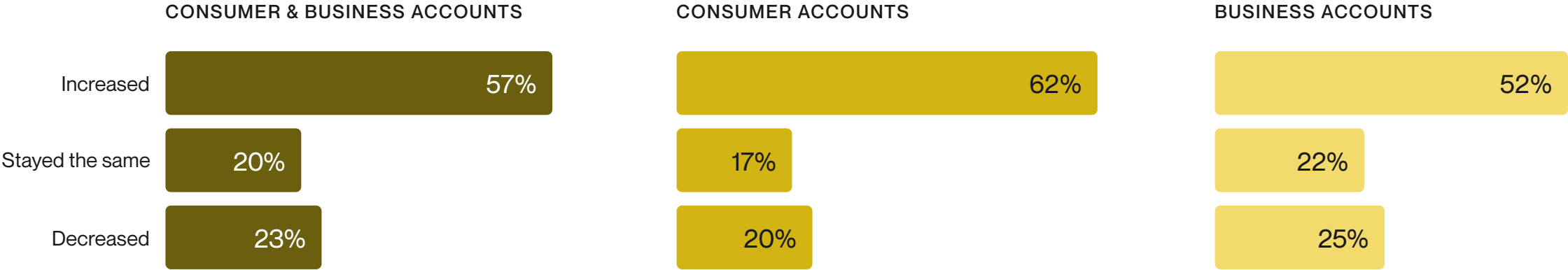
# Fraud trends in the US



# Fraud attacks are still increasing, but at a slower rate compared to last year.

 Alloy insight In 2022, 91% of respondents experienced an increase in fraud attacks. Although there was a significant decrease in 2023, over half of respondents still reported an increase in attempted fraud attacks. Encouragingly, 23% of respondents said fraud attacks decreased compared to just 1% last year.

How has the frequency of attempted fraud attacks in consumer/business accounts changed compared to last year?\*



Note: Frequency was framed differently in 2022 possibly leading to the disparity in attempted fraud attacks reported. 2022 survey options were: Increased significantly, Increased some, Neither increased nor decreased, Decreased some, and Decreased significantly

# Some sectors saw a decrease in attempted fraud attacks.

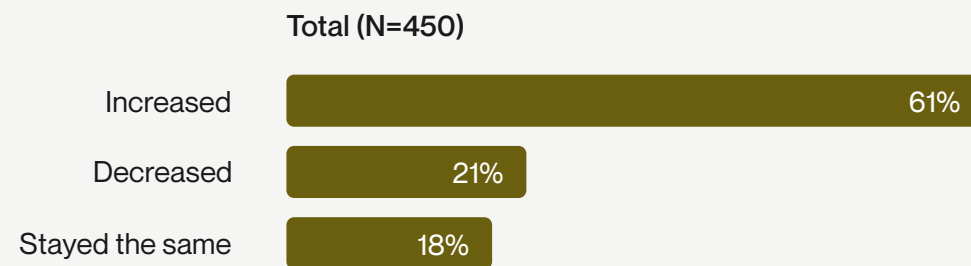
Combined US and UK data



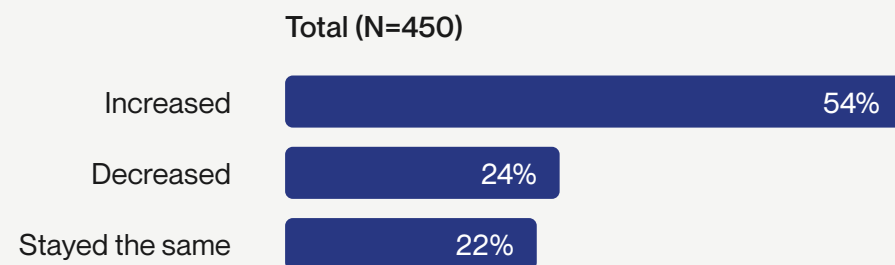
Alloy insight

Both enterprise fintechs and mid-market banks were more likely to say that fraud attacks decreased across both consumer and business accounts than the other segments.

How has the frequency of attempted fraud attacks in consumer accounts changed compared to last year?




How has the frequency of attempted fraud attacks in business accounts changed compared to last year?

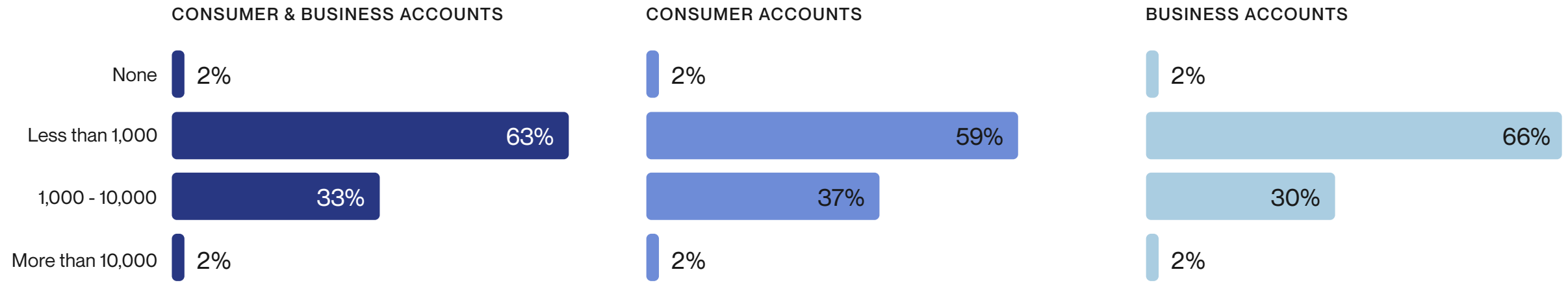


	FINTECH				BANKS				
	Growth fintech (N=15)	Strategic fintech (N=32)	Mid-market fintech (N=31)	Enterprise fintech (N=41)	Enterprise bank (N=68)	Mid-market bank (N=50)	Regional bank (N=43)	Credit union/Community bank (N=42)	Online/Pure pay lending (N=102)
Increased	80%	66%	68%	59%	56%	42%	74%	69%	58%
Decreased	20%	16%	3%	24%	13%	42%	9%	17%	31%
Stayed the same	0%	19%	29%	17%	31%	16%	16%	14%	11%
Small base size (<30)	73%	66%	52%	61%	46%	36%	63%	57%	54%
	13%	6%	3%	24%	21%	44%	16%	19%	32%
	13%	25%	45%	15%	34%	20%	21%	21%	14%

# In 2023, nearly all respondents experienced fraud, but they reported slightly fewer instances than the previous year.

 Alloy insight Roughly 35% experienced 1,000+ fraud attempts last year, down from 47% on average in 2022.

How many consumer/business accounts attempted to defraud your company in the past year?



# Manual fraud reviews were less common in 2023

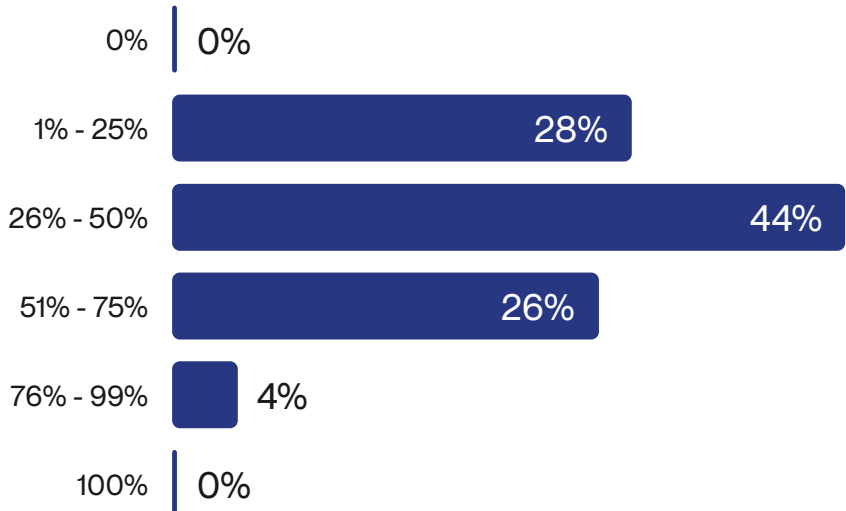
While manual reviews will always occur on some level, they are decreasing:

- 48% reported a decrease in manual reviews due to investments in fraud prevention tools.
- 65% said they manually review 26-50% fewer applications.

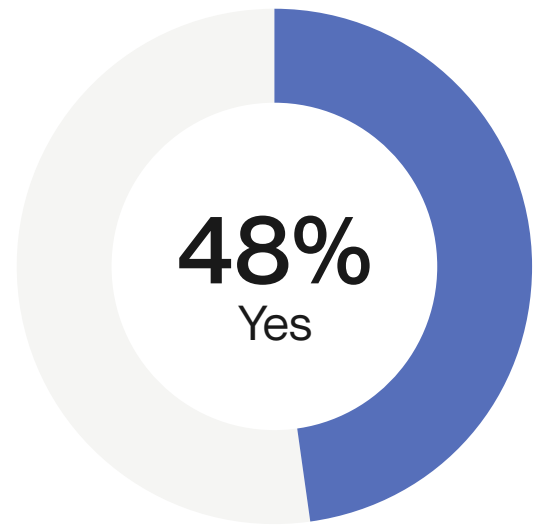
This indicates that organizations experienced tangible benefits as a result of fraud prevention tools.

**UK comparison:** UK respondents were more likely — 58% — to see a decrease in manual reviews as a result of fraud prevention tools.

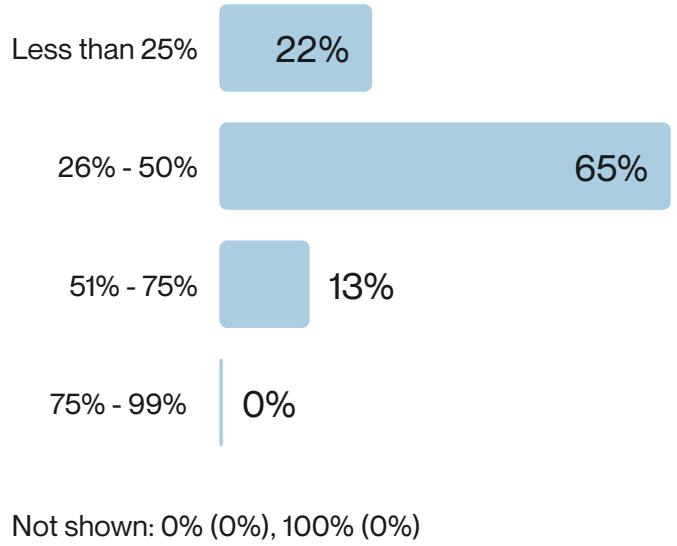
What percentage of new account applications require a manual fraud review by your analysts?



Has your investment in fraud prevention tools also led to a decrease in manual reviews?



Based on your response to the previous question, how much of a decrease?



# How are financial institutions and fintechs catching fraudsters?



## BENCHMARK

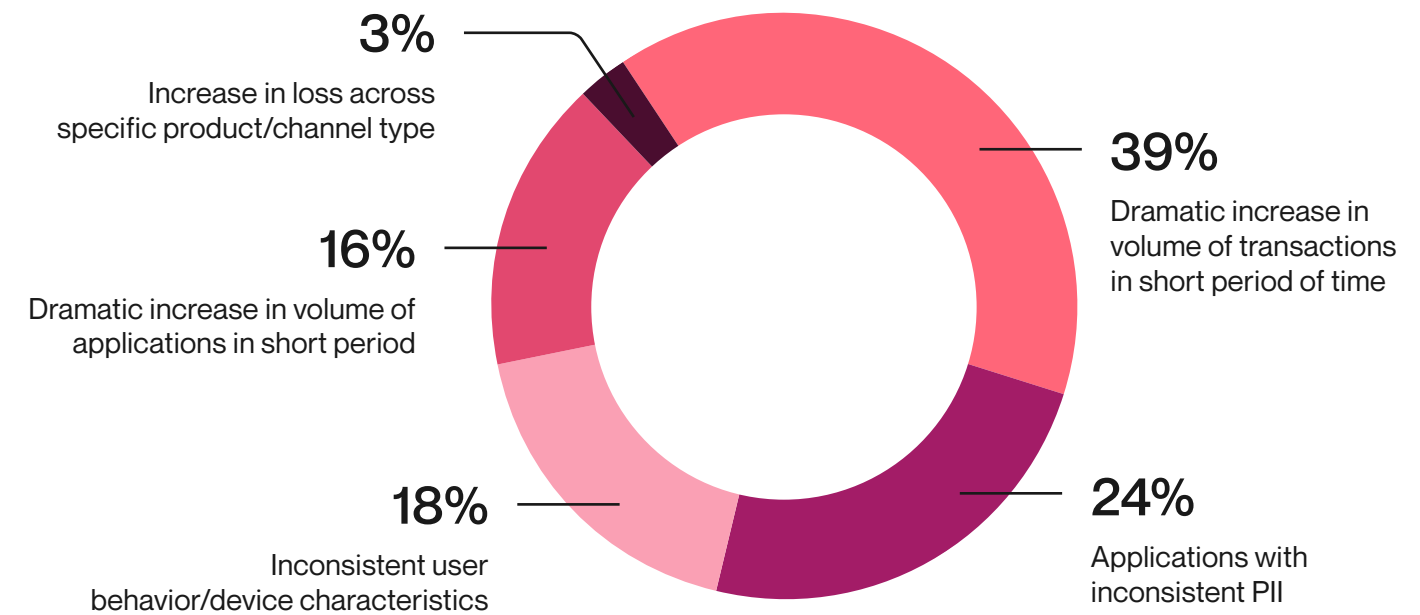
A “dramatic increase in volume of transactions in short period of time” is still the most common fraud indicator, with a 6% increase YoY.

The following changes were also statistically significant:

- 14% increase YoY in applications with inconsistent personally identifiable information (PII).
- 5% decrease YoY in the dramatic increase in volume of applications.

These stats indicate that fraudsters are turning to more sophisticated attack methods like identity theft as the use of AI in fraud prevention increases.

## What’s the most common flag when attempted fraud occurs?\*

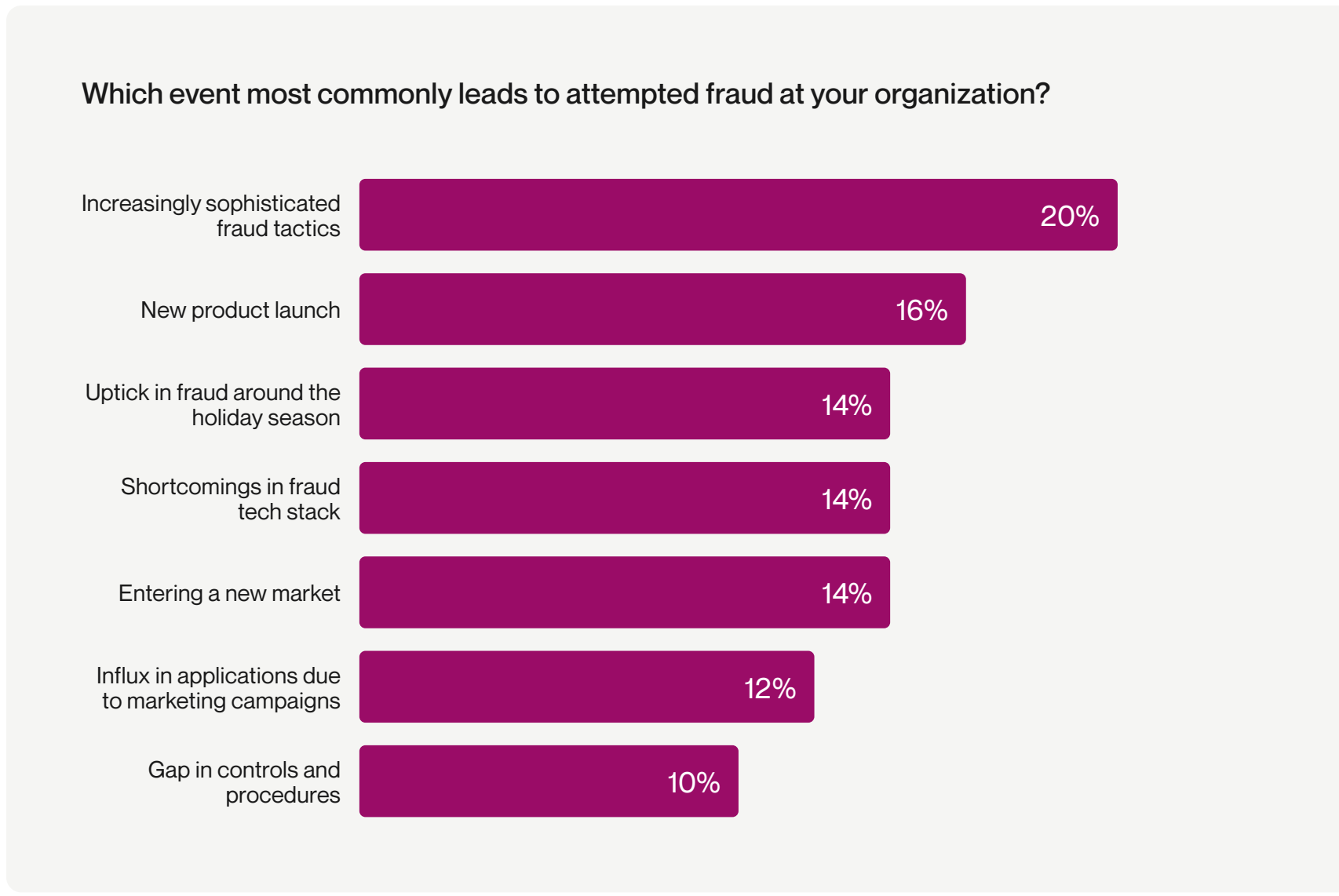


\*New in 2023: Dramatic increase in volume of transactions in short period of time, Increase in loss across specific product/channel type

\*Removed in 2023: High velocity of transactions, Dramatic increase in application approvals in short period of time

# More sophisticated fraud tactics appear to be on the rise.

The largest portion of respondents — 20% — reported that increasingly sophisticated fraud tactics are the leading cause of attempted fraud within their organization.



# Generally, respondents are still relying on real-time transaction monitoring to catch most fraud attempts.

 Alloy insight

50% of the respondents said they most commonly detect fraud in real-time, which was consistent with 2022 research. However, there was a 10% decrease YoY in their likelihood of detecting fraud at the time of onboarding. This could indicate organizations are relying too heavily on real-time transaction monitoring — even as attacks grow more sophisticated.

**UK comparison:** UK respondents are even less likely to commonly detect fraud during onboarding — only 18% compared to 33% in the US.

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

At time of transaction  
in real-time



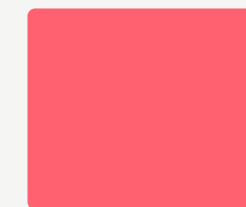
50%

At the time of  
onboarding



33%

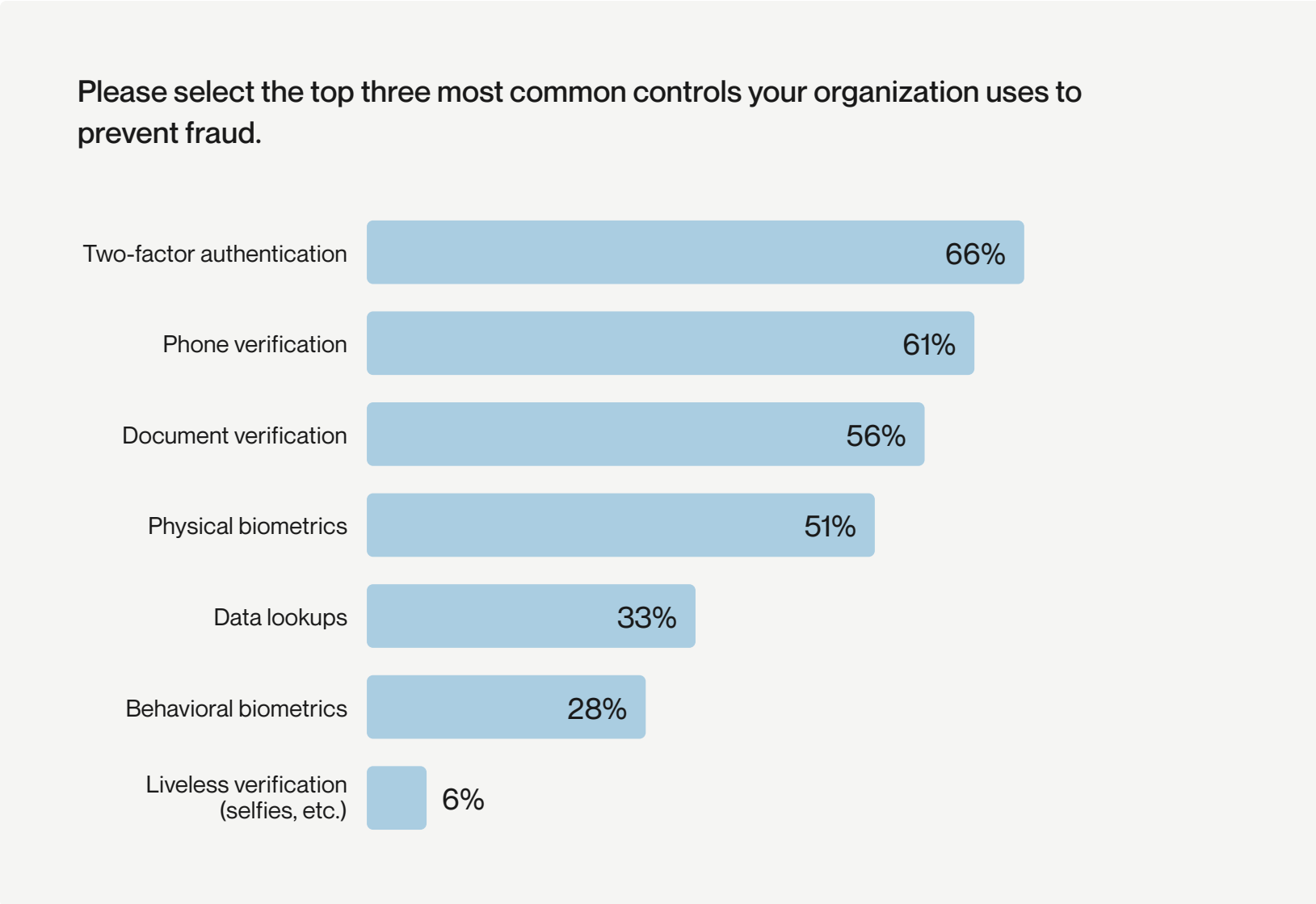
After transaction has  
occurred (after fraud  
has occurred)



17%

Not shown: Unable to determine (0%)

Two-factor authentication (2FA) is the most common control to prevent fraud before it occurs.





# When potential fraud is detected, step-up authentication is the most common action.

Combined US and UK data



## BENCHMARK

Generally, step-up authentication is the most popular course of action once an anomaly or risk is identified:

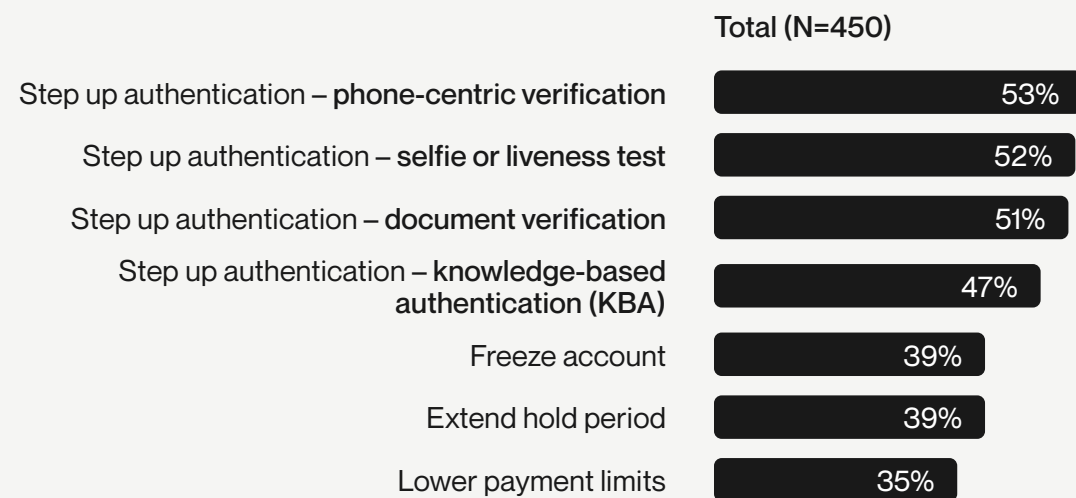
- The use of KBA increased considerably — 50% of respondents cited it as the first line of defense once fraud is detected, compared to 37% in 2022.
- The opposite occurred for document verification — 48% of respondents chose this response versus 63% in 2022.



## Alloy insight

Banks of all sizes were more likely to freeze accounts than fintechs. This trend may contribute to the perception that fintechs provide a better user experience than banks, which have recently come under fire for freezing or closing consumer accounts without warning.

### Once an anomaly or risk is identified, what do you do about it?

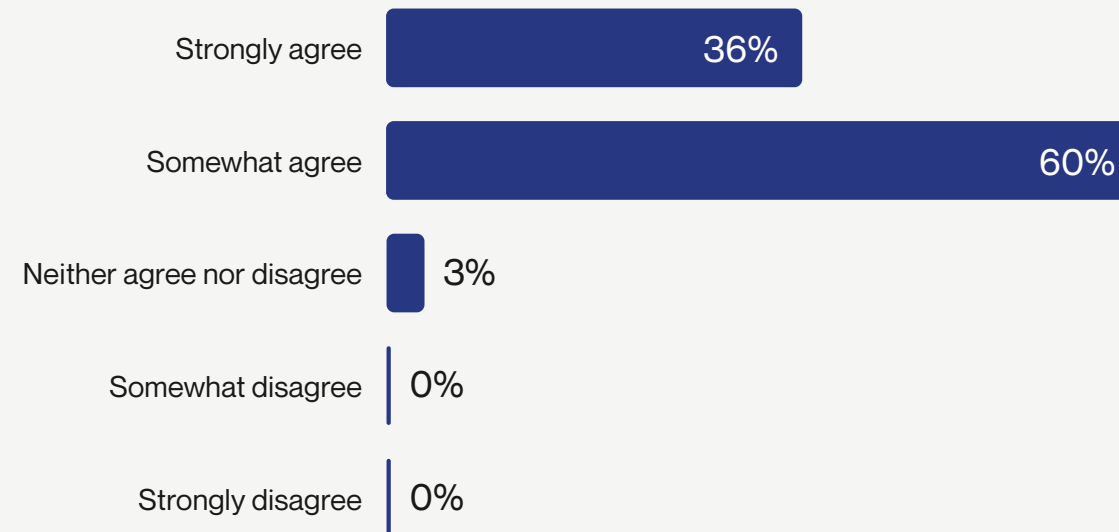


	FINTECH			BANKS					
	Strategic fintech (N=32)	Mid-market fintech (N=31)	Enterprise fintech (N=41)	Enterprise bank (N=68)	Mid-market bank (N=50)	Regional bank (N=43)	Credit union/Community bank (N=42)	Online/Pure pay lending (N=102)	
<b>Growth fintech (N=15)</b>	47%	45%	39%	56%	38%	37%	64%	69%	
	44%	26%	59%	53%	40%	40%	62%	65%	
	53%	45%	49%	59%	36%	44%	40%	64%	
	38%	45%	41%	37%	46%	47%	48%	65%	
	34%	19%	39%	53%	70%	51%	40%	17%	
	16%	52%	22%	44%	52%	42%	43%	36%	
	47%	42%	41%	47%	40%	30%	24%	25%	
<b>Small base size (&lt;30)</b>									

# How are organizations preventing fraud?

Nearly all of the respondents — 96% — believe their organization can handle increasing fraud threats. Yet, the majority — approximately 60% — only somewhat agree, which indicates an underlying sentiment that their organization still has room to improve their fraud management practices.

How strongly do you agree or disagree with the following statement about your organization?  
“Our organization is sufficiently equipped to respond to growing fraud threats.”

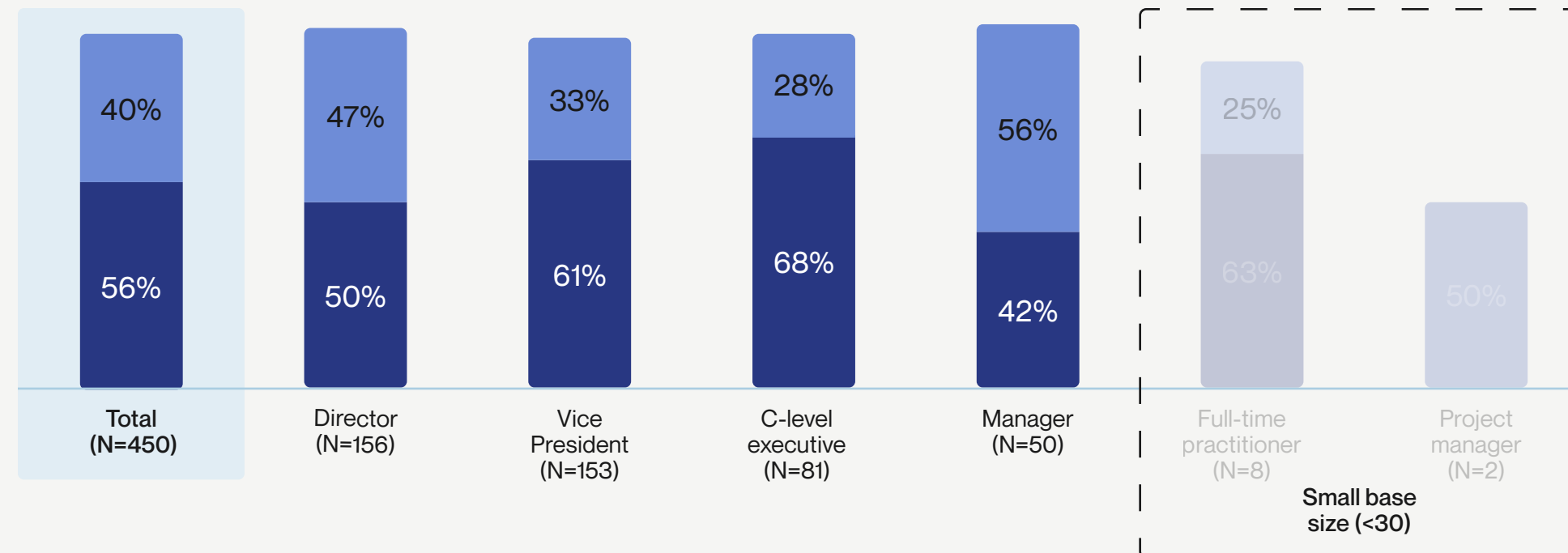


# Across the US and the UK, organizations are confident in their ability to respond to growing fraud threats.

Combined US and UK data

How strongly do you agree or disagree with the following statement about your organization?  
“Our organization is sufficiently equipped to respond to growing fraud threats.”


■ Somewhat agree ■ Strongly agree



## 💡 Alloy insight

The more senior their role, the less likely respondents were to strongly agree that their organization is sufficiently equipped to deal with growing fraud threats.

# Most organizations are optimizing their existing fraud models.

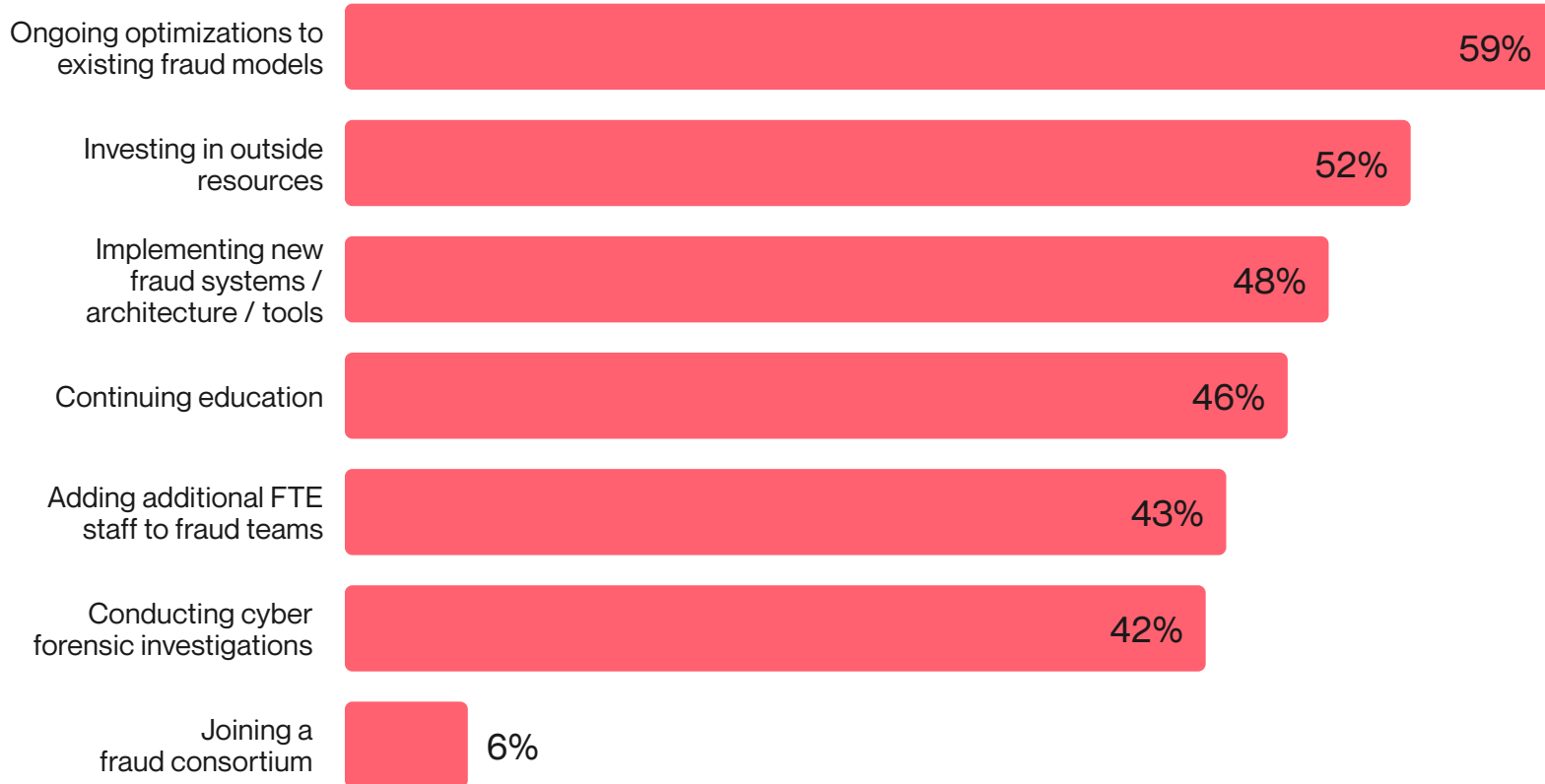
 BENCHMARK

Beyond using in-line controls, **59%** of respondents indicated that their organizations focus on enhancing current fraud prevention models.

It's worth noting that approximately **52%** allocated funds to external resources to combat fraud, a significant rise from the **40%** in 2022.

**UK comparison:** In the UK, the majority of respondents — **58%** — indicated they were more likely to add additional FTE staff to fraud teams.

Outside of in-line controls\*, what kinds of fraud prevention measures is your company taking?\*\*\*



\*In-line controls are defined as measures and safeguards integrated directly into operational processes or systems to prevent, detect, and mitigate fraudulent activities in real-time.

\*\*Slight variations in question text and/or answer option wording vs. 2022

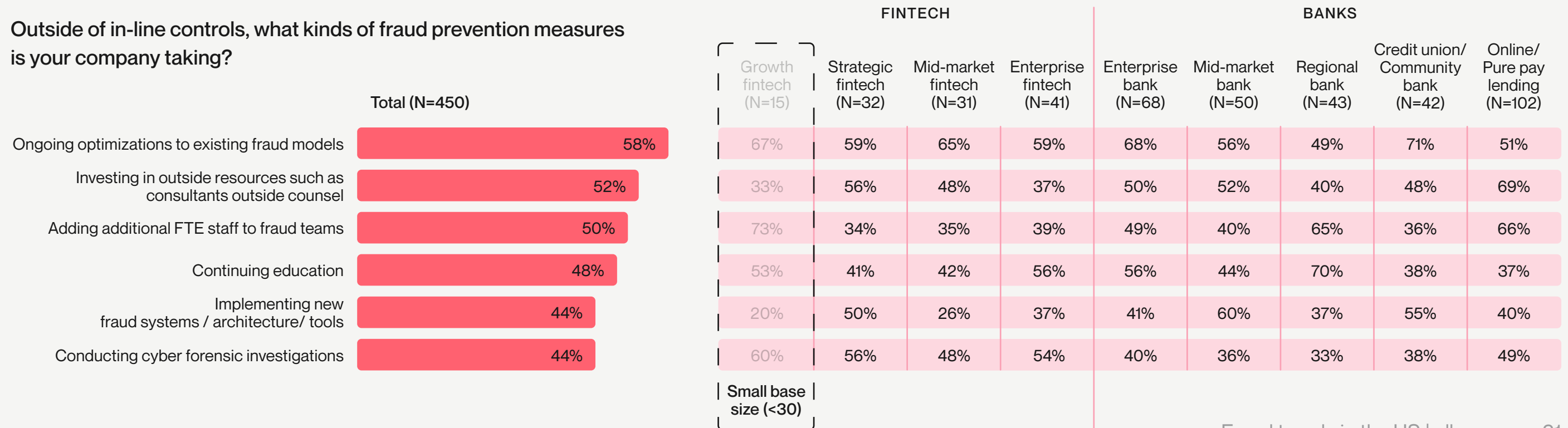
Not shown: Other (0%), None of the above (0%)

# Credit unions and community banks are most likely to optimize their existing fraud models.

Combined US and UK data

**Alloy insight** 60% of mid-market banks reported they were implementing new fraud systems — higher than any other segment. The mid-market bank segment also had the highest percentage of respondents report a decrease in fraud over the past 12 months (at 43%, see page 10). This might indicate that companies that look beyond just the optimization of their legacy fraud models could see more success in decreasing their overall fraud volume.

## Outside of in-line controls, what kinds of fraud prevention measures is your company taking?





# The continued overreliance on KBA will lead to lost opportunities to catch fraud throughout the customer lifecycle.

The use of knowledge-based authentication (KBA) increased considerably, even though **20%** — the largest portion of respondents — said that increasingly sophisticated fraud tactics lead to attempted fraud within their organization.

It comes as a surprise to many that KBA questions are often actually easier for a fraudster to answer than the average legitimate consumer. While a legitimate customer will often forget their answers, fraudsters will work to gain access and tend to be able to find the answers through simple internet searches.

In other words, banks and fintechs are using a relatively unsophisticated authentication option like KBA even though they are being confronted with increasingly sophisticated fraudsters, and they have become less likely to detect fraud.

Amid the rapid increase of fraud attacks in 2022, hasty investments — or a lack of investments in advanced fraud prevention tools — might have led to a reliance on tools like KBA, even though it is easily circumvented by fraudsters and creates friction and inconveniences legitimate users.

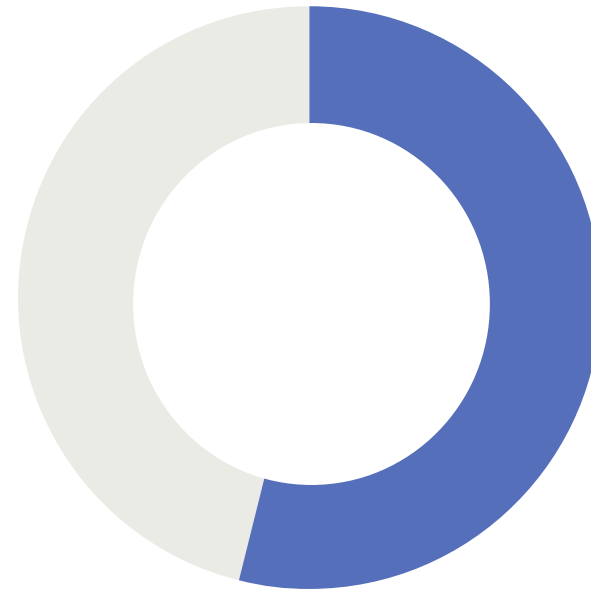
Which is all to say, the overreliance on KBA could backfire in the long run. This signals a need for fraud solutions that are both more effective and user-friendly — especially if most companies are seeking to update their existing fraud models.

# Most organizations conduct real-time interdiction on transactions and/or applications.

Approximately 96% of respondents conduct some form of real-time interdiction.

In the US, larger organizations with 1,001+ employees are more likely to conduct real-time interdiction on applications than smaller firms.

However, less than half of respondents claimed to conduct real-time interdiction on applications. This demonstrates a remaining need for stronger investments in robust fraud prevention solutions that leverage the capabilities of real-time interdiction, so more fraud can be stopped at origination.



**54%**

conduct real-time interdiction on transactions



**42%**

conduct real-time interdiction on applications

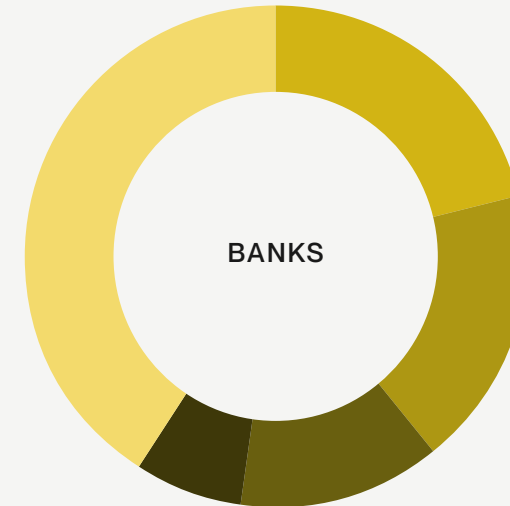
Not shown: No, but plan to (4%), No, not planning on it (0%)

# Mobile drives the most fraud challenges for both banks and fintechs.

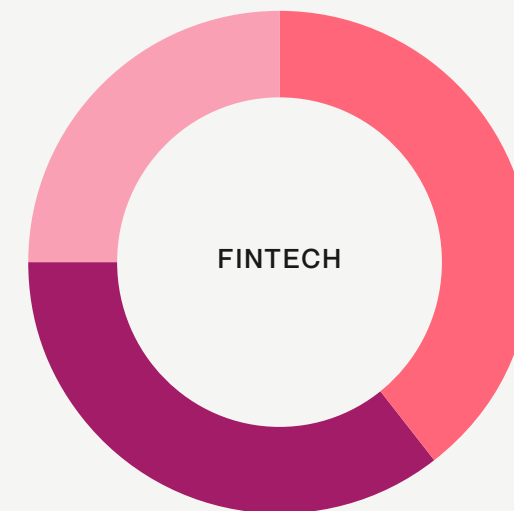
Combined US and UK data

Overall, respondents mostly encounter fraud via internet-based platforms such as mobile and online/digital services. Mobile channels are equally prominent in facilitating fraudulent activities in both fintech and traditional banking.

On which channels is fraud most commonly occurred?



- Mobile banking (41%)
- Online banking (21%)
- Branch (18%)
- ATM (13%)
- Contact center (7%)

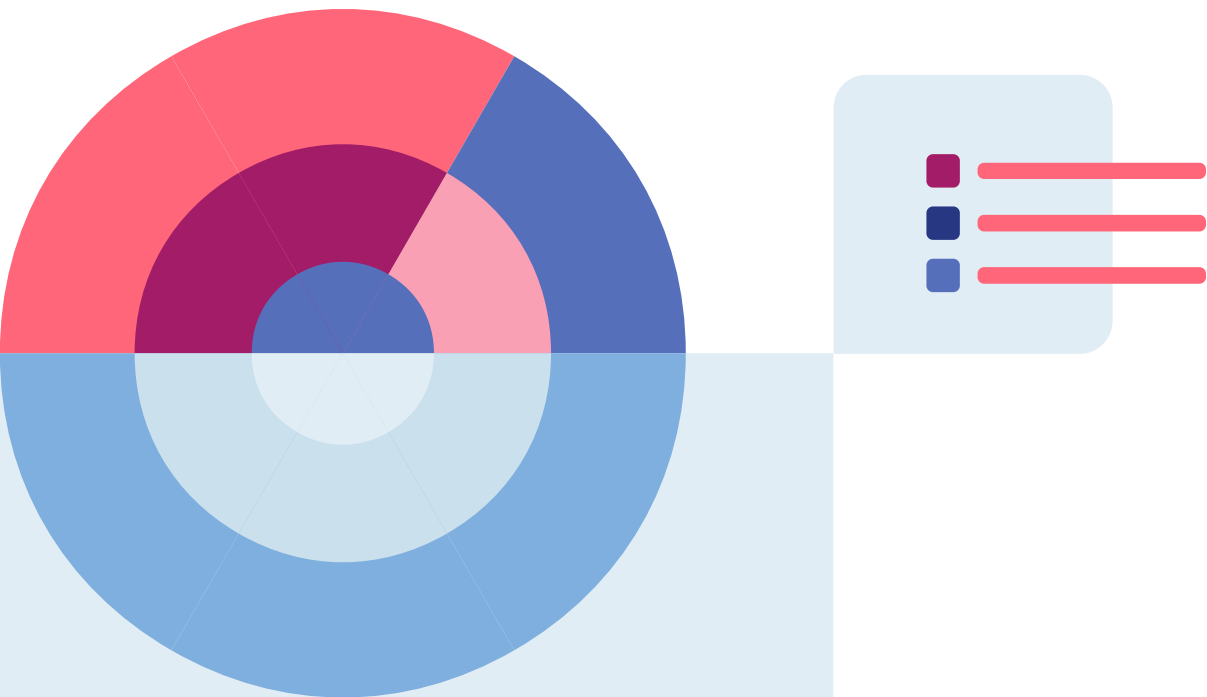


- Contact center/Customer service (25%)
- Mobile (39%)
- Online/Digital (35%)





# Transaction-centric fraud reporting leads to difficulties tracking fraud across channels.



Online and mobile banking made up approximately **62%** of fraud attempts reported by US-based banks and **75%** of fraud attempts reported by fintechs, while human touchpoints, like contact centers and banking branches, accounted for just **25%** of those attempts.

- Due to the human component, it's likely that fraud attempts are not always tracked well. They are often attributed to the channel of execution, instead of the channel where the fraudster originated.
- For example, if fraud originates at a contact center but is executed online, it is likely that this fraud will be classified based on the channel of execution (online), not the channel of origination (human touchpoint).
- The channel where the actual loss occurs still leads the organization's fraud classification, but additional information about where the fraud originated is beneficial to correctly classify the fraud type
- Correct classification is more likely to help prevent fraud at origination versus the attempt to mitigate and further prevent fraud after a transaction has taken place.



# Transaction-centric fraud reporting leads to difficulties tracking fraud across channels.

*cont.*

This speaks to a need for broader fraud education, both within the industry and outside of it, to grasp the multifaceted nature of fraud and to avoid oversimplified fraud prevention tactics like adding KBA questions or freezing accounts.

As organizations invest in more controls digitally, fraudsters will shift their attention to exploiting vulnerabilities in other channels unless organizations begin to use an omnichannel approach to fraud prevention.

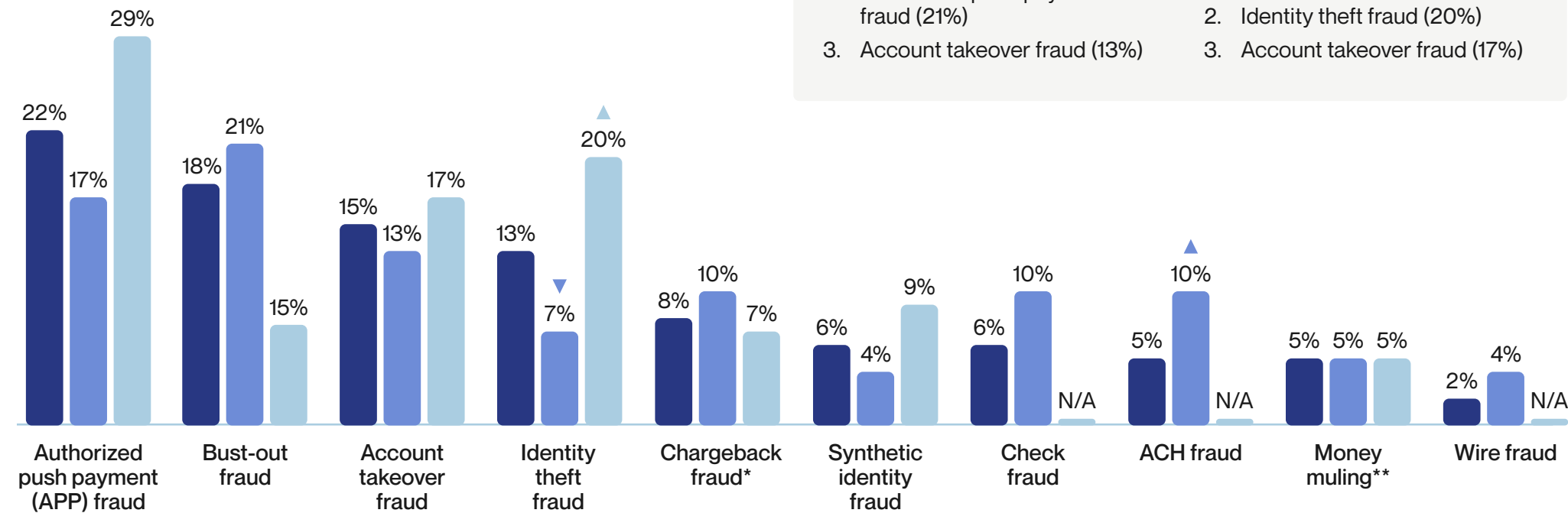
The complexity of fraud models, and their underlying identity-related issues, necessitates a deeper understanding and more nuanced approach for effective prevention and mitigation that does not result in increased customer friction.

# Authorized push payment fraud is the most common type of fraud, universally.

Combined US and UK data

What type of fraud do you see most frequently by case volume?

■ Total 
 ■ US 
 ■ UK 
 ▲▼ Indicates statistically higher or lower than the total at 95% confidence



## Alloy insight

While authorized push payment (APP) fraud was the most common type of fraud for US and UK respondents combined, it is more common in the UK compared to the US — 29% versus 17% respectively. However, when you look at the US alone, bust-out fraud is the most common type of fraud at 21%.

UK participants are about twice as likely to report identity theft as the most prevalent form of fraud relative to US respondents — 20% versus 7%.

\*\*“Friendly fraud” displayed to UK respondents  
 \*\*\*“Coercion fraud” displayed to UK respondents

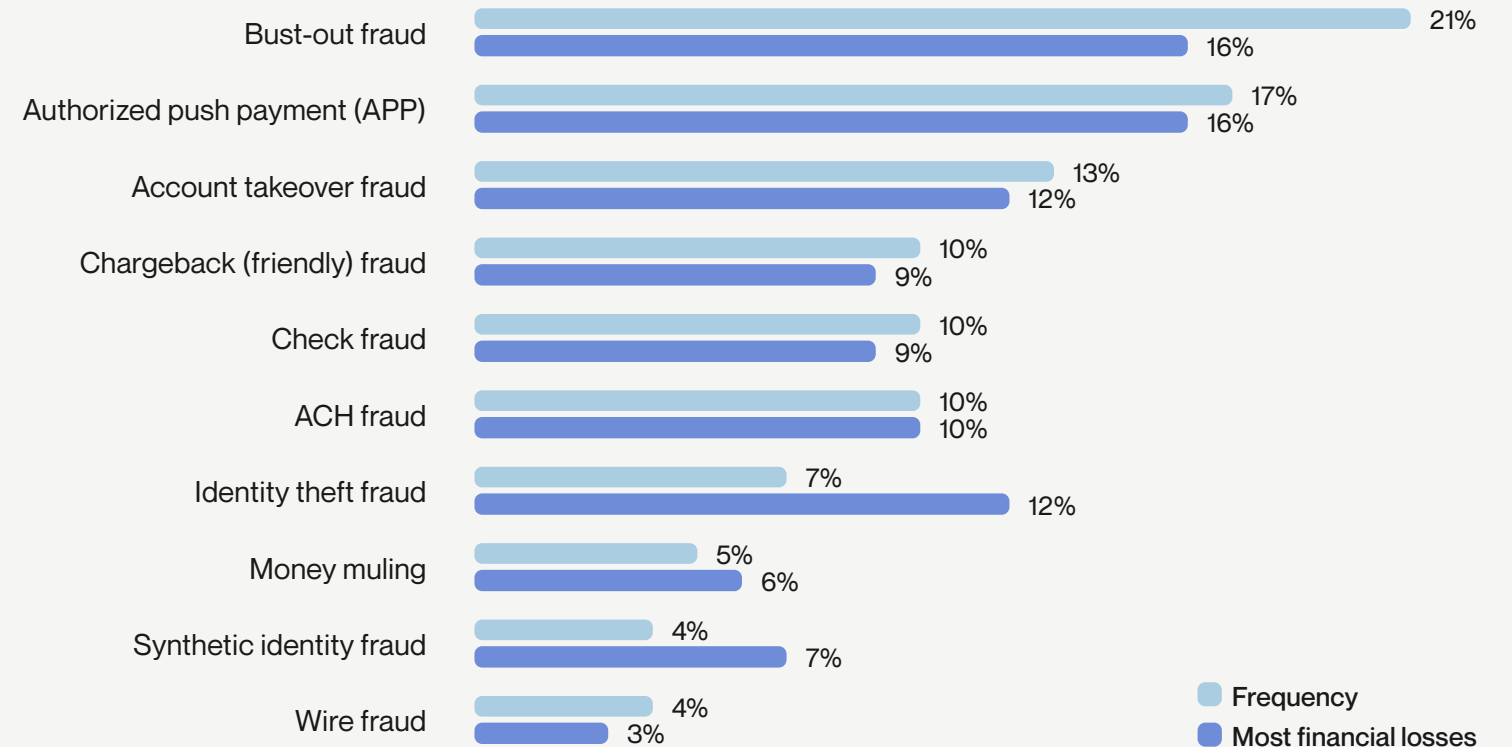
# The types of fraud that occur most often are also the ones that tend to cause the most financial damage.



Bust-out fraud and APP fraud are the most common; they also cause the most financial damage for organizations.

While identity theft is not as frequently occurring as other types of fraud, the financial burden it brings can be equally severe. This number could be low due to lack of identifying and/or reporting a case as identity theft. In other words, organizations classify and report a fraud event, such as bust-out or account takeover fraud, but might not report that there was also an associated identity theft.

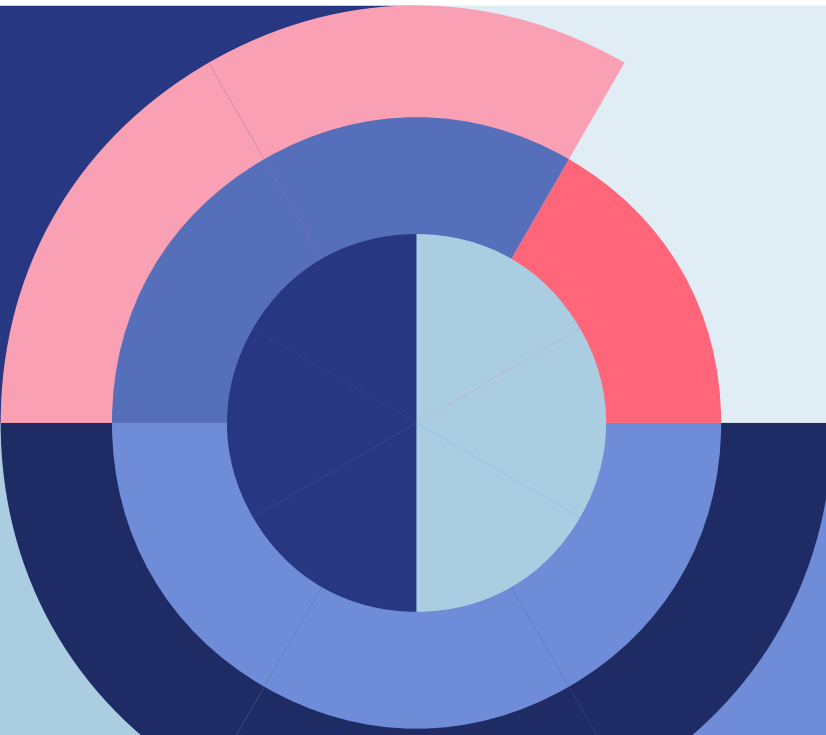
What type of fraud is most prevalent by frequency / financial losses?



Note: "Friendly fraud" & "Coercion fraud" not displayed, only shown to UK respondents.



# Banks and fintechs struggle to define and categorize fraud, but they need to get better — and fast.



To mitigate fraud, banks and fintechs must be able to clearly identify both the type of fraud methodology being used and the channel where it's originating.

- For example, APP fraud was universally named as the most common type of fraud — but it is also one of the easiest to identify.

In 2024, if organizations want to keep pace with fraudsters, this means shifting the focus from fraudulent transactions to fraudulent identities.

Fraud prevention should not be a one-size-fits-all approach. Most banks and fintechs are in need of a strategic pivot to omnichannel solutions. This will allow them to innovate and use a wider variety of fraud methodologies as needed across different channels to address their unique vulnerabilities as they arise.

Identity Risk Solutions may play a crucial role in curbing proportional spikes in synthetic identity fraud, potentially leading to loss reductions.



# Instances of synthetic identity fraud are likely being underreported.

Last year, Alloy's experts predicted that the personally identifiable information (PII) stolen in early 2020 would surface in 2023-2024 — exactly three years after the leaks.

- Synthetic identities are usually built over the span of multiple years, as fraudsters “warehouse” the stolen information and build their fake identities’ credit history for 3-5 years before using it to apply for accounts.
- When institutions are focused solely on fraudulent transactions instead of fraudulent identities, they could be giving these fraudsters more opportunity to “bust out” and steal a larger amount of funds.

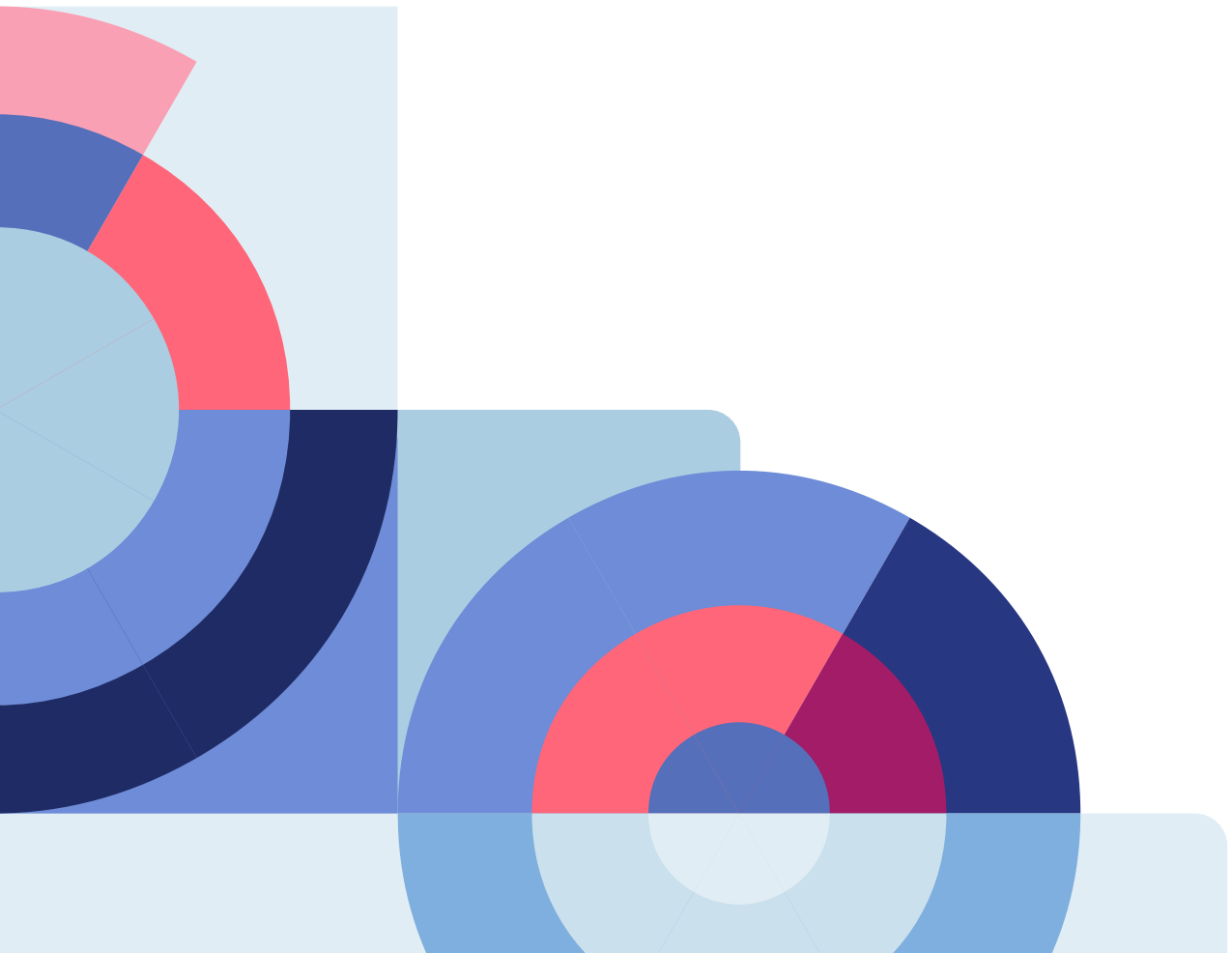
In a continuation of this trend, applications with inconsistent PII increased **14% YoY — 24% in 2023 versus 10% in 2022.**

- This could indicate an increase in synthetic fraud, which is often mislabeled as first-party, friendly, or chargeback fraud — a repeated trend from 2022.





# Instances of synthetic identity fraud are likely being underreported. *cont.*



This year's survey presented more answer options for fraud types compared to last year's in an effort to aid respondents' fraud classification. While the challenge of labeling continues, we can look to the US and the UK's differences to see where synthetic identity fraud may have gone unreported.

- Bust-out fraud was singled out as the most common type of fraud by case volume in the US at **21%**.
- In the UK, participants were twice as likely to report identity theft as the most prevalent form of fraud relative to US respondents — **20% versus 7%**.
- This indicates that fraud teams in the US are more likely to focus on the method of execution rather than the type of fraud being committed, which leads to less of a focus on identity and less targeted prevention strategies.

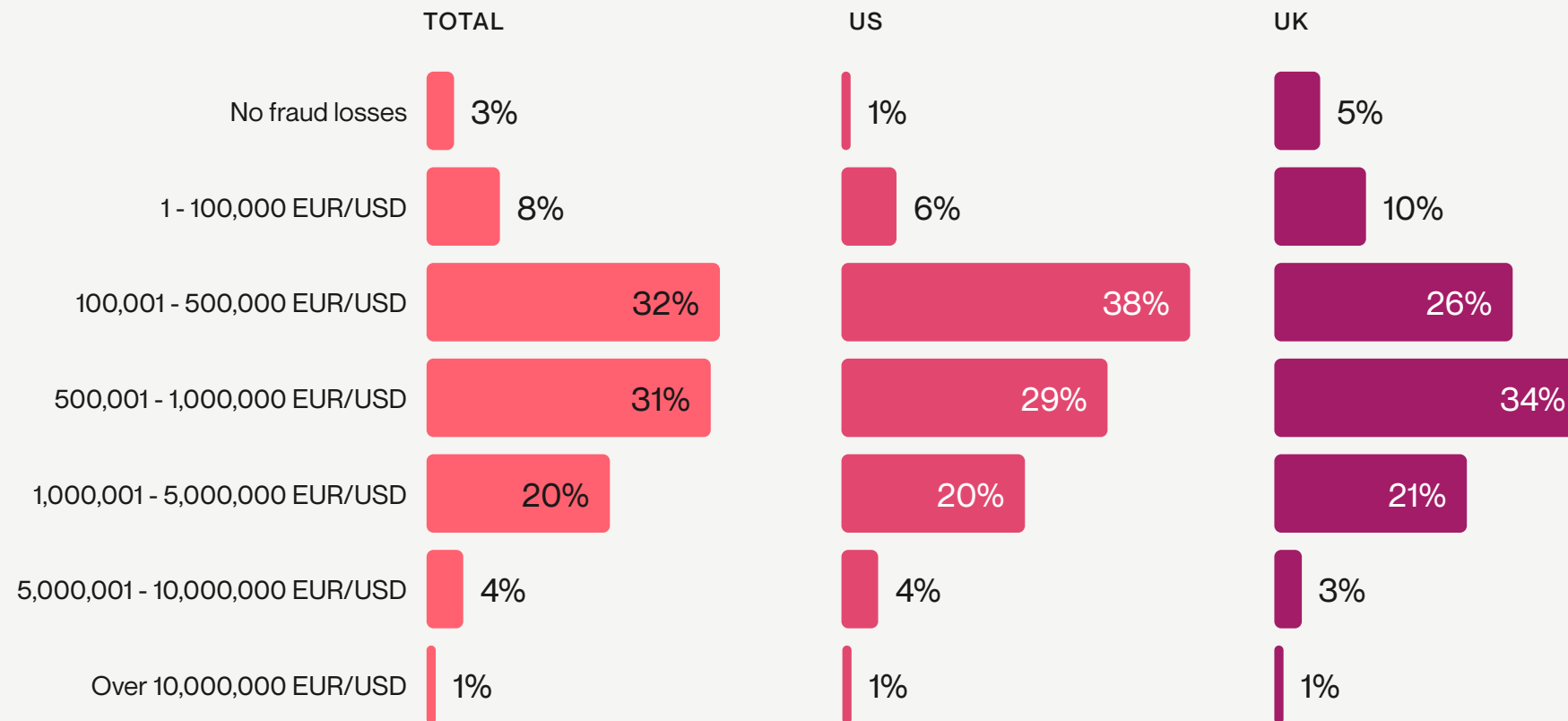
# The cost of fraud in the US



# The direct cost of fraud

Combined US and UK data

How much do you think your organization may have incurred in direct fraud losses over the last 12 months?



Not shown: Don't know/not sure (Total – 1%, US – 0%, UK – 2%)  
 Note: No significant differences by country.

 Alloy insight

Respondents in both the US and the UK suffered significant financial losses due to fraud:

- 56% of respondents lost more than 500,000 EUR/USD to fraud in the last 12 months.
- In that same time period, 25% lost over 1 million EUR/USD.

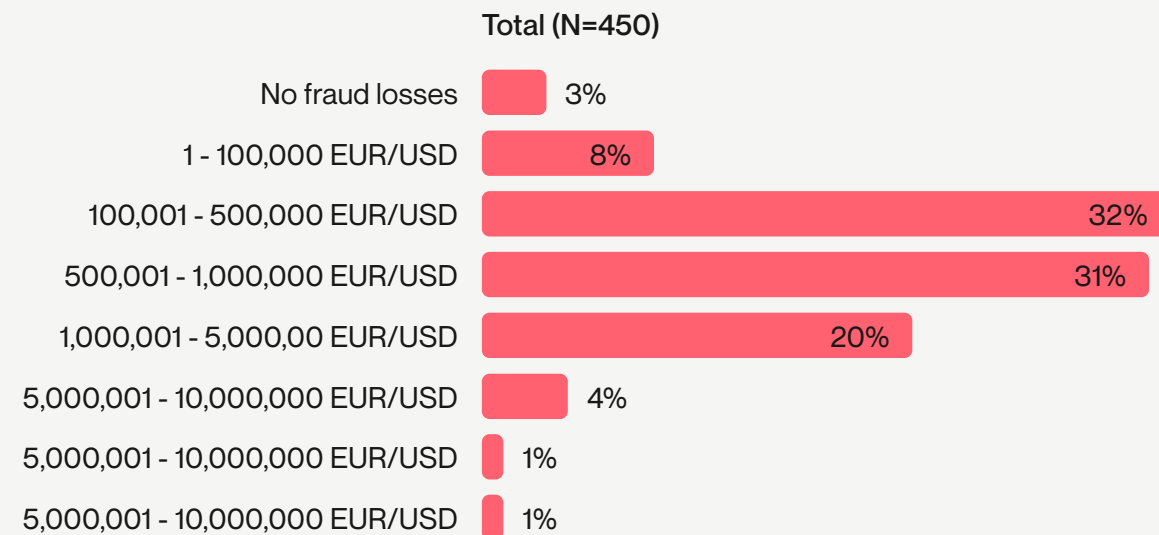
# Direct fraud losses add up faster for smaller organizations

Combined US and UK data

**Alloy insight** A large portion of companies lost over \$500K to fraud. 79% of credit unions and community banks reported more than \$500K in direct fraud losses – higher than any other segment.

Fraud losses particularly hurt smaller businesses like credit unions/community banks and mid-market fintechs, which underscores the importance of managing fraud in tightening macroeconomic conditions.

## How much money has your organization incurred in direct fraud losses over the last 12 months?




	FINTECH			BANKS					
	Growth fintech (N=15)	Strategic fintech (N=32)	Mid-market fintech (N=31)	Enterprise fintech (N=41)	Enterprise bank (N=68)	Mid-market bank (N=50)	Regional bank (N=43)	Credit union/Community bank (N=42)	Online/Pure pay lending (N=102)
Small base size (<30)	33%	0%	6%	0%	4%	0%	2%	2%	0%
	13%	22%	6%	17%	4%	8%	2%	5%	5%
	27%	22%	13%	20%	29%	34%	63%	14%	38%
	13%	28%	42%	24%	34%	26%	14%	29%	46%
	13%	28%	29%	39%	18%	28%	7%	38%	9%
	0%	0%	3%	0%	9%	2%	2%	10%	2%
	0%	0%	0%	0%	1%	2%	2%	2%	0%
	0%	0%	0%	0%	0%	0%	7%	0%	0%

# Despite decreased losses, US-based banks, fintechs, and credit unions were less successful at recovering those funds compared to last year.

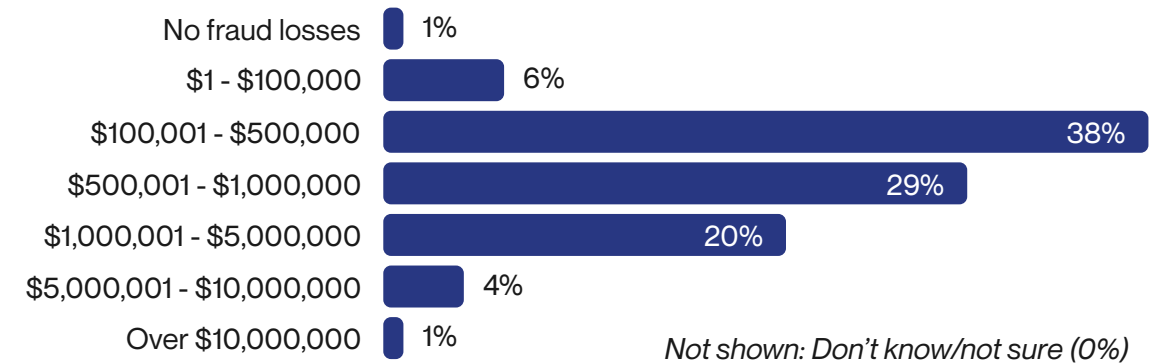
 Alloy insight

It is worth noting that institutions have become more strict on their process for the returning of funds, which can directly impact the amount that can be recovered.

 BENCHMARK

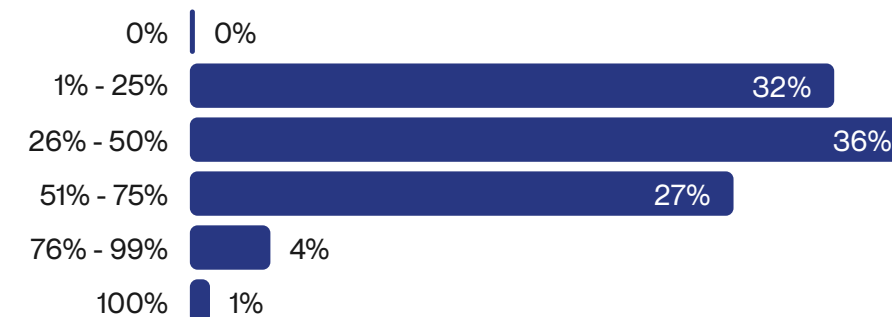
Overall, US participants experienced fewer financial setbacks compared to 2022. More respondents reported losses ranging from \$100,000 to \$500,000 rather than \$500,000 to \$1,000,000, which marks a reversal from the previous year's trend.

How much money has your organization incurred in direct fraud losses over the last 12 months?



However, fewer respondents were able to recover these losses. Approximately 32% said they were able to recover 50%+ in fraud losses, a drop from 66% in 2022.

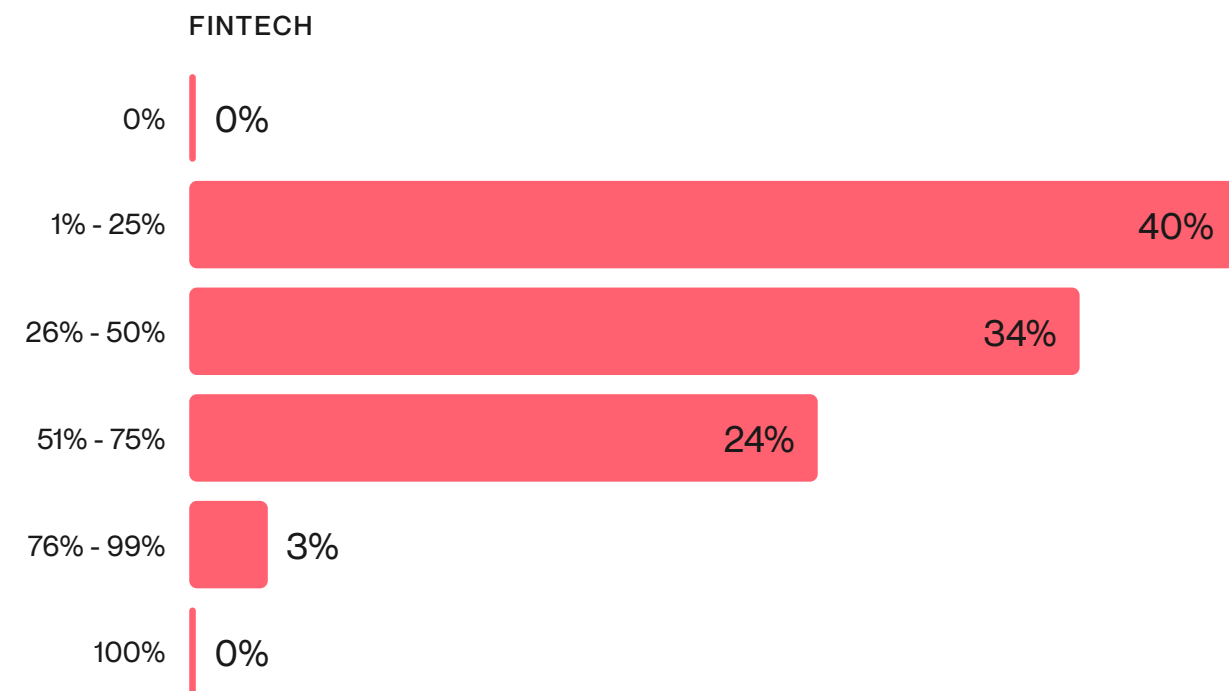
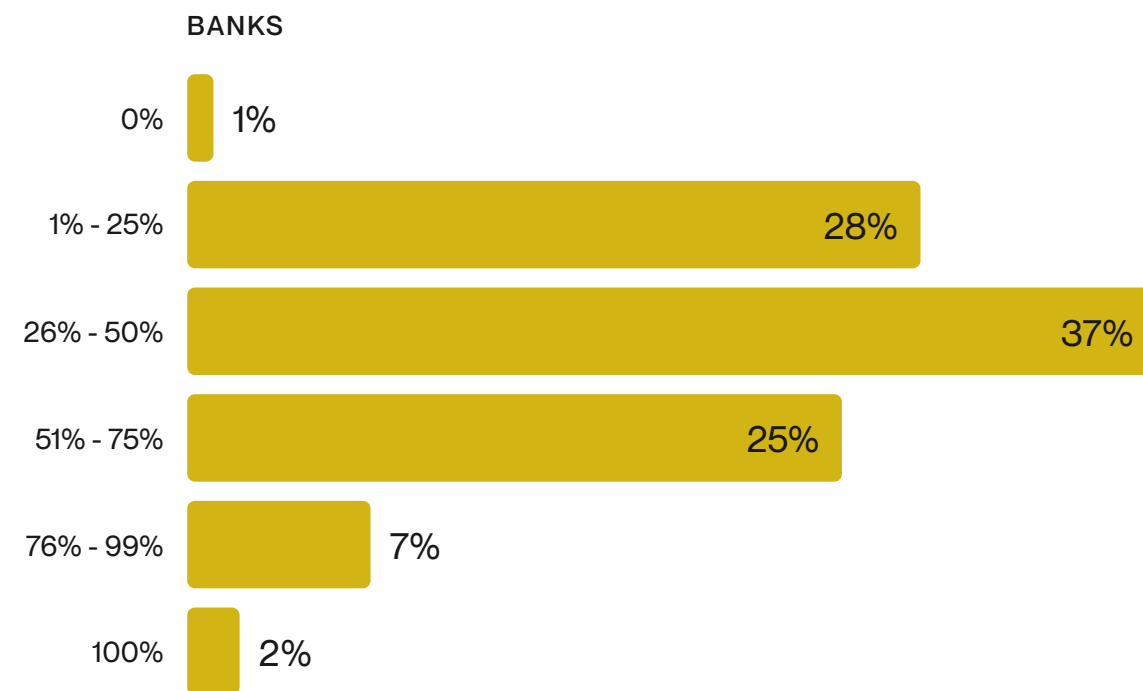
Approximately how much of these fraud losses were recovered?



# In general, banks in both the US and the UK were more successful than fintechs at recovering stolen funds.

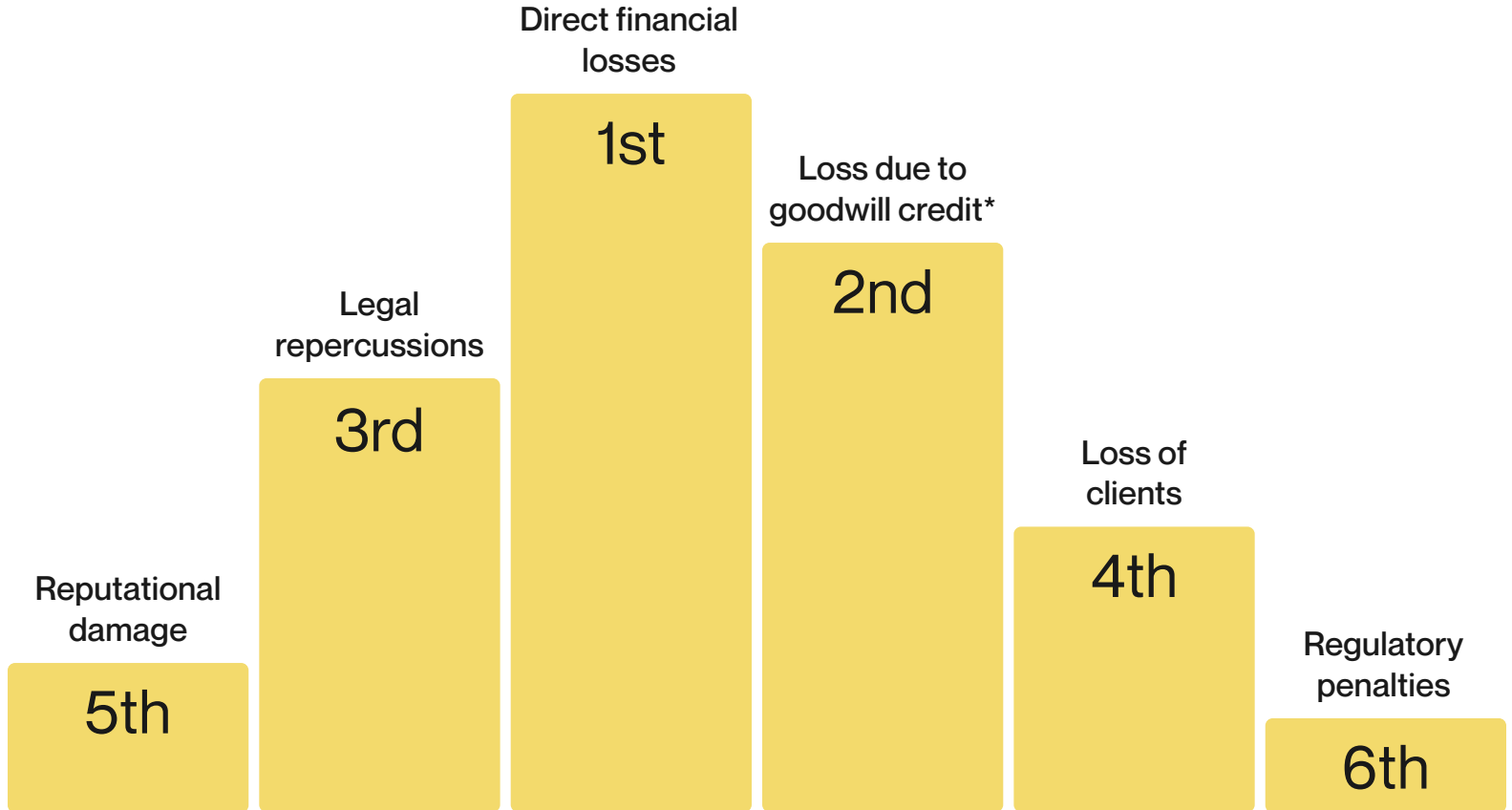
Combined US and UK data

Approximately how much of these fraud losses were recovered?



# Not all costs are treated equally, and direct financial losses emerged as a big concern in the US.

Please rank the following consequences of fraud from 1 – most consequential to 6 – least consequential?



\*Added in 2023  
 Chart displays choices in order from highest percentage ranked number 1 to lowest

**BENCHMARK**

Respondents deem “direct financial loss due to fraud” as the biggest consequence of fraud, consistent with 2022.

In 2023, Alloy added a new option — “Loss due to goodwill credit” — which ended up ranking second overall.

# Not all costs are treated equally

Combined US and UK data



## Alloy insight

Last year, C-suite executives were more likely to rank reputational damage first, and loss of clients second. This year, they shifted to ranking direct financial losses first, which could indicate increased pressure to meet their company's bottom line amidst tightening macroeconomic conditions.

## What is the most consequential impact of fraud?

	Total (N=450)	Director (N=156)	Vice president (N=153)	C-level executive (N=81)	Manager (N=50)	Full-time practitioner (N=8)	Project manager (N=2)
Direct financial losses	41%	35%	48%	36%	40%	63%	100%
Loss due to goodwill credit to client	17%	16%	18%	17%	20%	0%	0%
Legal repercussions	12%	12%	14%	15%	6%	13%	0%
Reputational damage	12%	16%	8%	9%	16%	0%	0%
Loss of clients	11%	12%	9%	15%	8%	13%	0%
Regulatory fines/penalties	7%	10%	3%	9%	10%	13%	0%

Small base size (<30)

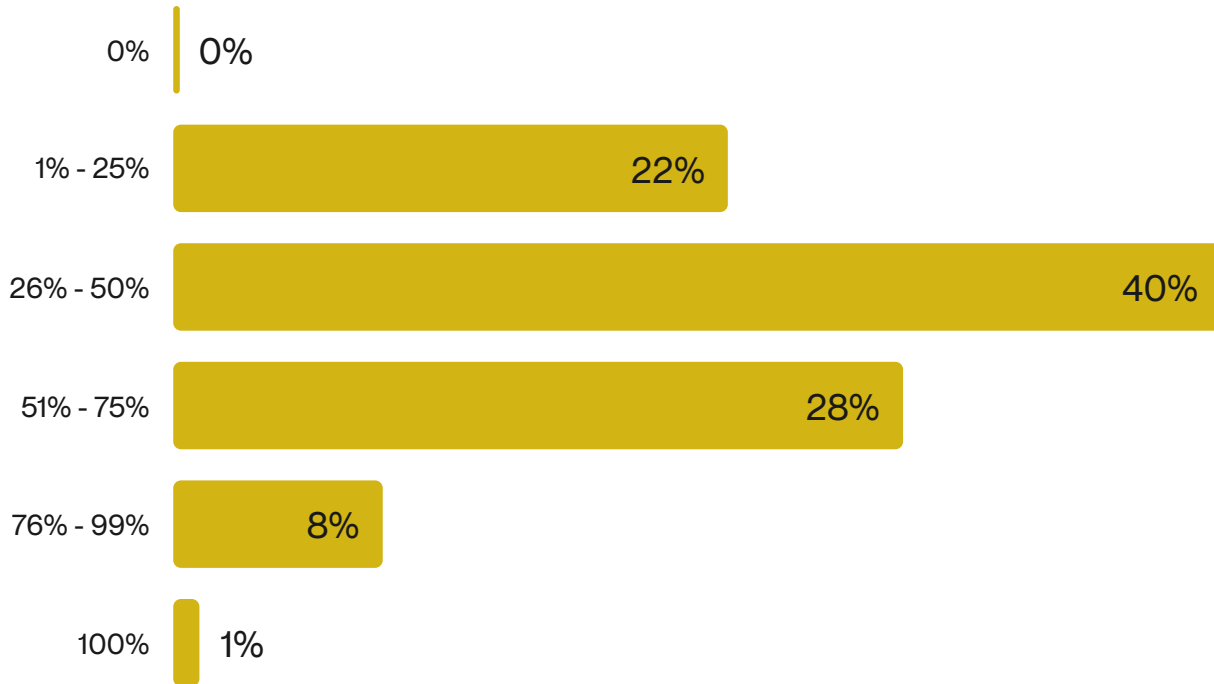
# How many developers does it take to solve fraud?

 BENCHMARK


Only 37% of respondents said that more than half of their development teams are focused on fraud-related activities.

As fraud has slowed, and financial losses from fraud attacks have decreased, companies are getting more comfortable outsourcing fraud prevention and re-allocating their internal resources.

What percentage of your development teams are focused on fraud-related activities?



# US financial institutions and fintechs continue to view fraud prevention as a worthwhile investment.

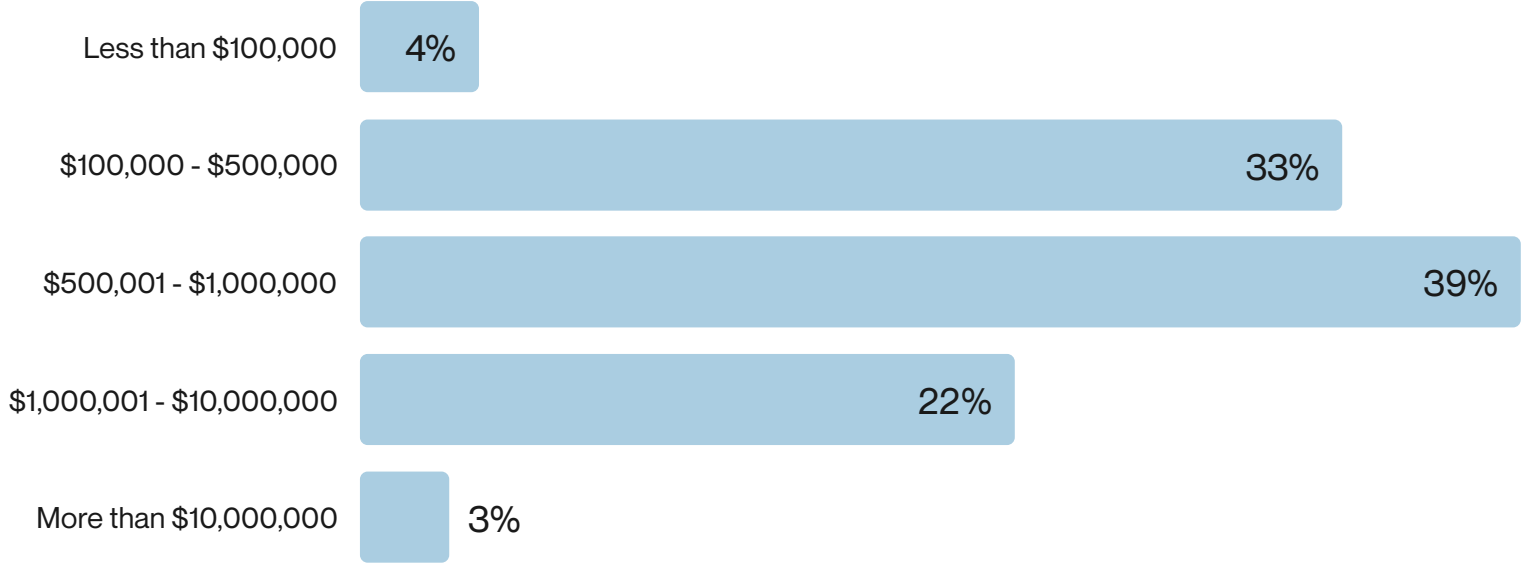
 BENCHMARK

The largest portion of respondents spent an estimated \$500,000 - \$1,000,000 on fraud prevention in 2023. This included investments in their fraud tech stack, labor required to recover and prevent fraud losses, regulatory fines, and goodwill credits to customers.

Larger organizations of over 1,000 employees generally spend more.

Though only 54% of respondents said they lost over \$500,000 to fraud, 64% are spending over \$500,000 on fraud prevention.

How much do you estimate your organization has spent on fraud prevention in the past 12 months?



Not shown: Unable to determine (0%)



# Fraud predictions for 2024

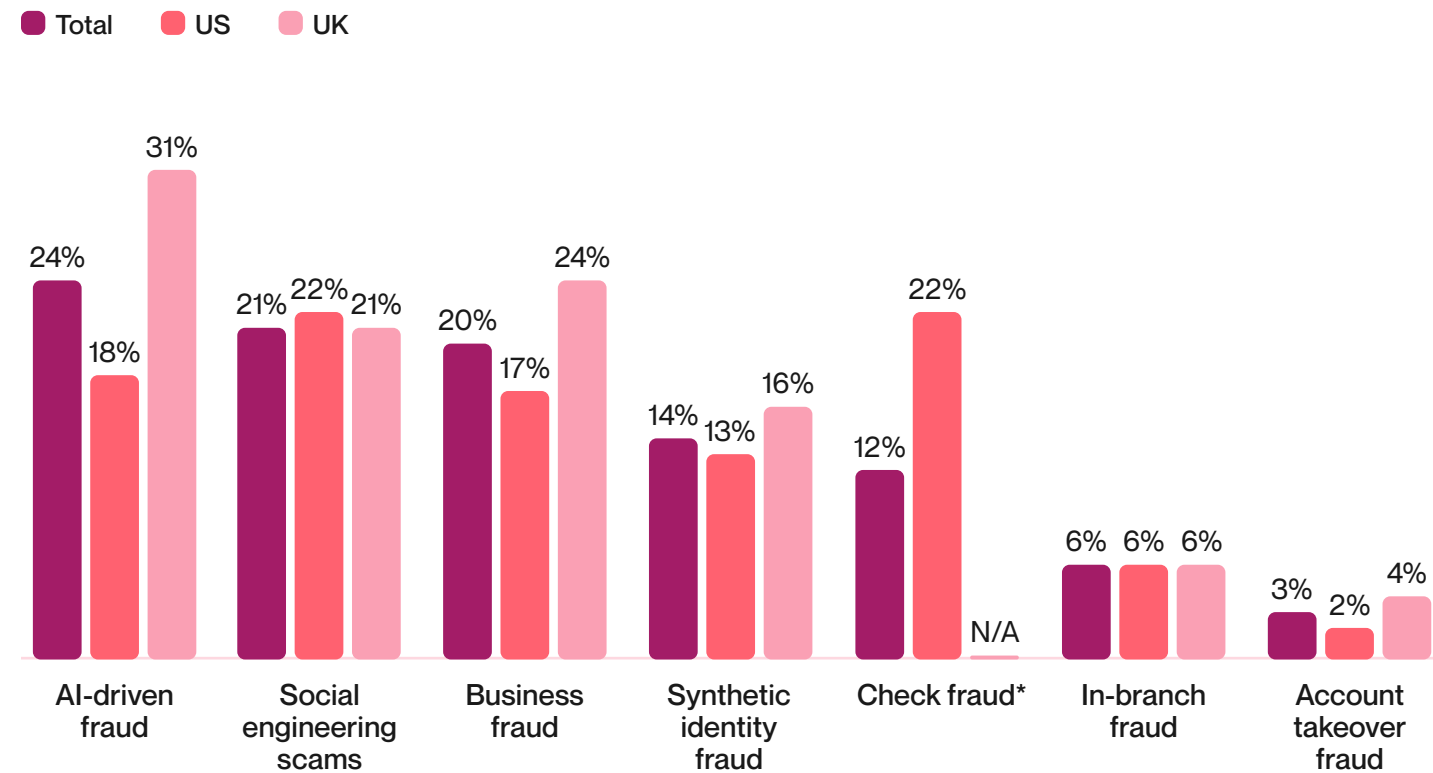
# Check fraud and social engineering scams are US respondents' primary fraud concerns for 2024.

Combined US and UK data

Both US and UK respondents addressed their fraud concerns for the coming year:

- US respondents are most focused on social engineering scams and check fraud.
- While social engineering scams remain a significant concern across the pond, UK respondents were more concerned with AI-driven fraud compared to US respondents.

What emerging fraud trend are you most concerned about in the coming year?



\*Check fraud not shown to UK respondents due to it not being applicable in that geographical area

# Looking ahead in 2024, both banks and fintechs are exploring investments in more agile fraud prevention solutions.

What types of technologies will you be looking to invest in the next 12 months?



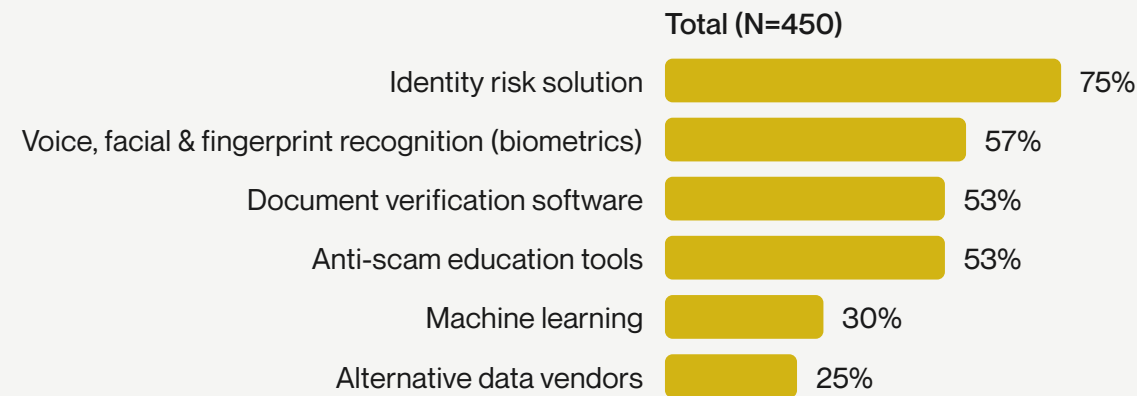
The majority of US respondents responded that they are looking to invest in an Identity Risk Solution within the next 12 months.

**BENCHMARK**

## US and UK investments in fraud prevention technology

Combined US and UK data

What types of technologies will you be looking to invest in the next 12 months?



Small base size (<30)	FINTECH			BANKS					
	Growth fintech (N=15)	Strategic fintech (N=32)	Mid-market fintech (N=31)	Enterprise fintech (N=41)	Enterprise bank (N=68)	Mid-market bank (N=50)	Regional bank (N=43)	Credit union/Community bank (N=42)	Online/Pure pay lending (N=102)
	73%	66%	55%	66%	74%	70%	60%	88%	87%
	60%	56%	29%	44%	62%	66%	63%	55%	62%
	60%	59%	65%	54%	66%	50%	42%	43%	52%
	40%	44%	81%	51%	59%	54%	47%	55%	48%
	27%	34%	19%	27%	28%	40%	58%	26%	15%
	27%	22%	29%	41%	25%	16%	9%	29%	29%



# Increased investment in agile, flexible fraud solutions is helping to combat growing fraud rates.

A majority of respondents (**57%**) agreed fraud attacks increased compared to last year — down from **91%** saying fraud rates increased YoY in last year's report — indicating that overall fraud is still increasing, just at a slower, less noticeable pace than 2022.

In last year's report, **71%** of survey respondents indicated an increase in their fraud prevention spending during 2022.

- This likely drove the **12%** decrease YoY of respondents who experienced more than 1,000 fraud attempts in 2023 — and the slower growth of fraud attacks in general.

This suggests that the countermeasures being put into place are working and will continue to drive results.

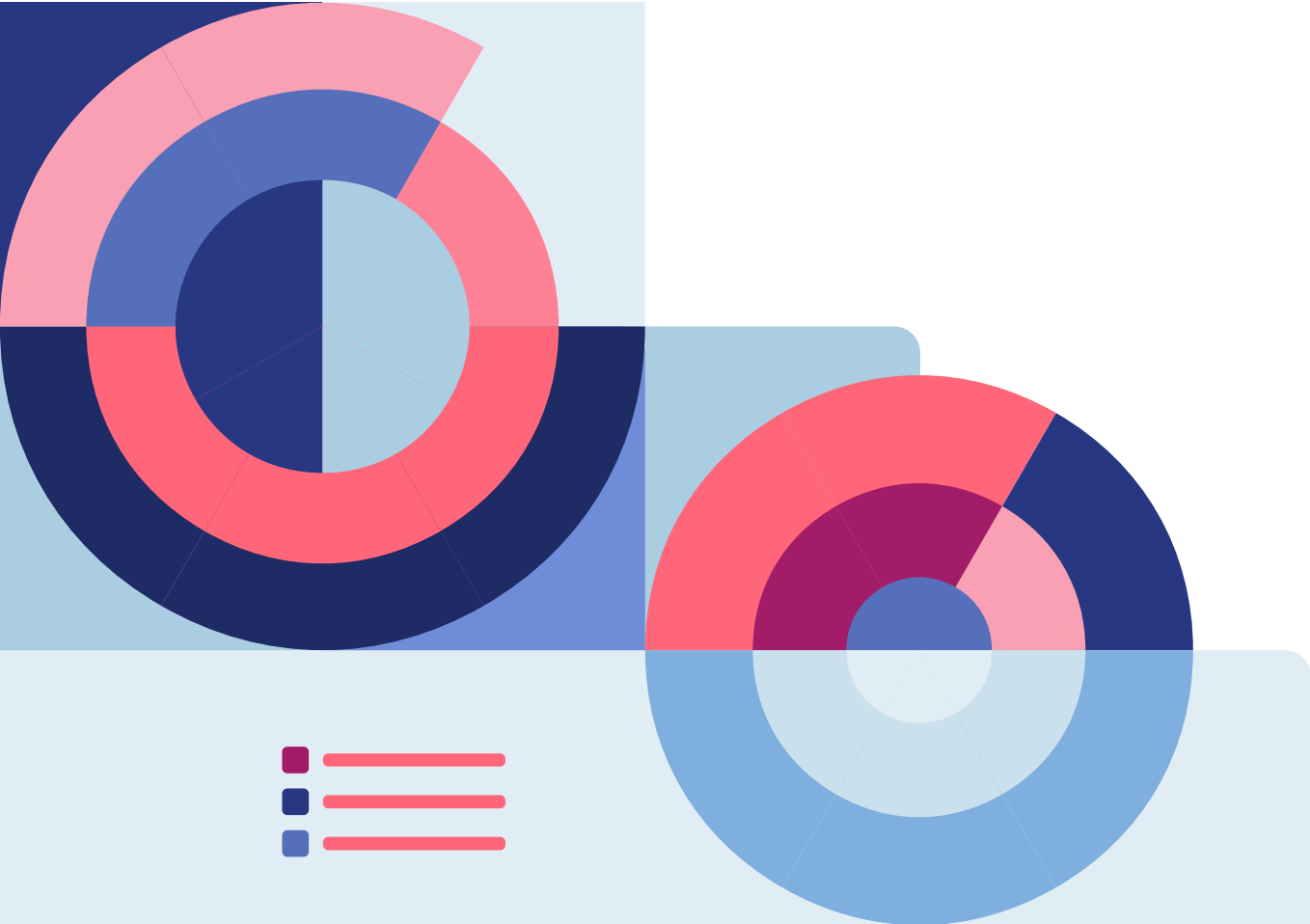
- Hence, the **12%** uptick in the investments that organizations are making in outside resources — from **40%** in 2022 to **52%** in 2023.

Respondents also stated that they plan to continue making significant investments in fraud prevention technology, which could be an indicator that fraud prevention attempts have been successful as manual reviews have decreased.

- **75%** of respondents said they were looking to invest in an Identity Risk Solution in the next 12 months — a **16%** increase YoY — in 2023.

# Where will fraud go next in 2024?

A prediction from Alloy's CEO, **Tommy Nicholas**



## On AI

It's important to note that third-party predictive models have actually utilized machine learning for over a decade to help banks and fintechs solve identity risk. As more fraudsters use AI to perpetuate their crimes, it has also become clear that the key to responding to new AI-born threats isn't as simple as using more AI. Instead, we saw and will continue to see more companies adopting a holistic approach to fraud prevention and mitigation that leverages behavioral analytics, biometrics, and the third-party predictive models that already employ machine learning.

On the other hand, also expect a rise in AI-driven fraud driven by things like FraudGPT. Fraudsters are resourceful, and they will use this technology to enact increasingly sophisticated scams. In response, banks have already begun implementing better scam-education tools and fraud prevention protocols.

# Where will fraud go next in 2024?

Predictions from **Sara Seguin**,  
Principal Advisor of Fraud & Identity Risk



### On open banking

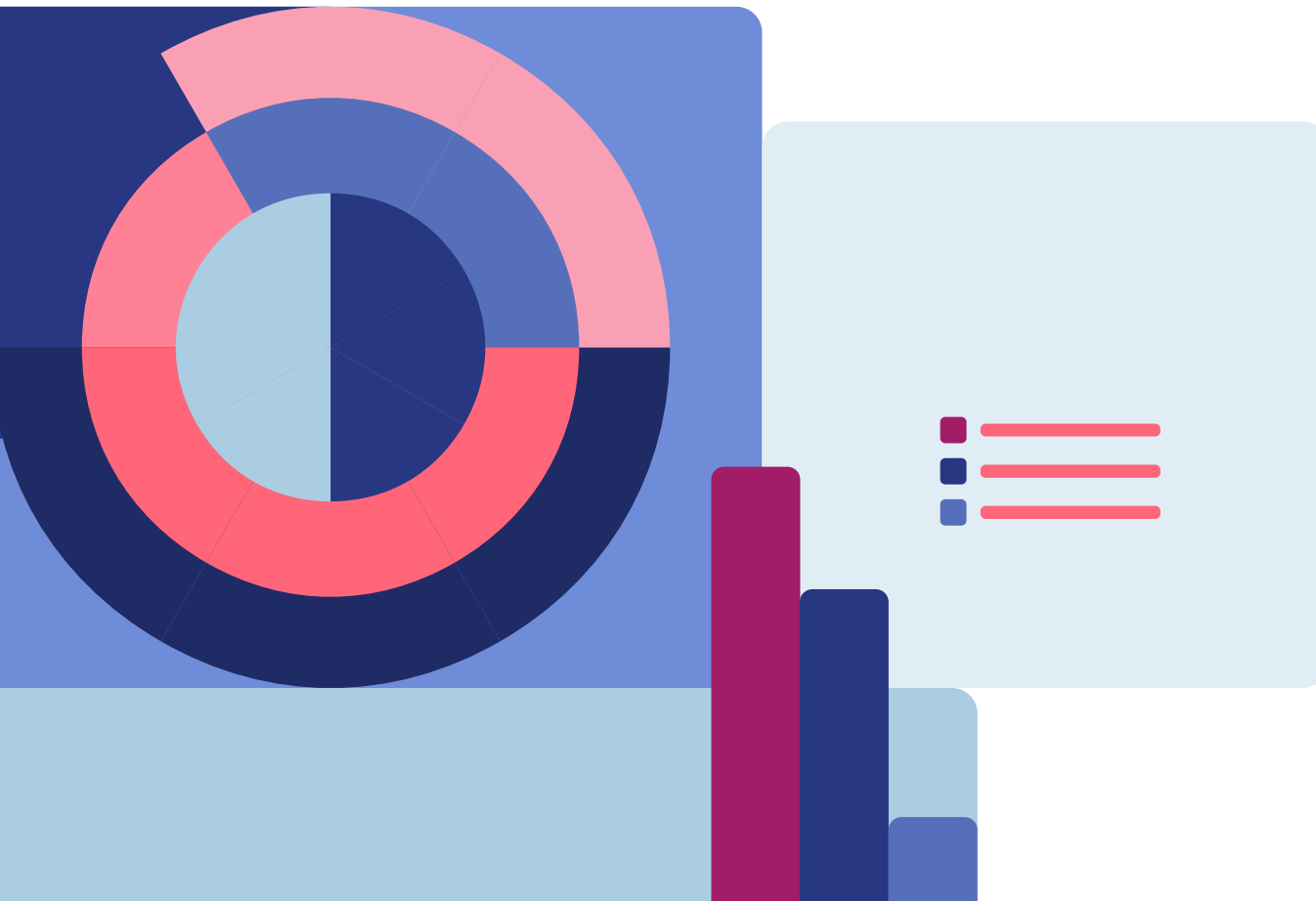
Since open banking enables consumers to share financial information across apps and services, more inroads are created for fraudsters to break in and get a comprehensive look at consumers’ financial data. To reduce their exposure to these kinds of attacks, I anticipate more banks will invest in onboarding controls, so that their fraud teams can identify fraudulent accounts at origination. We’ll also see increased monitoring throughout the customer journey, verifying third-party apps and services they allow to connect to a bank’s system along the way.

### On FedNow

A lot of banks have been taking a wait-and-see approach with FedNow. But in the next year, it will increase its user base in a few key sectors. As more customers embrace faster payment rails, fraud attempts will also grow faster and increase. Fraudsters will find new ways to exploit digital payments, including increasingly sophisticated account takeover attacks. Again, banks and fintechs will need to establish strong controls at onboarding — as well as rules and interdiction that are set up to identify account takeover — as part of their transaction monitoring processes.

# Where will fraud go next in 2024?

Predictions from **Sara Seguin**,  
Principal Advisor of Fraud & Identity Risk



## On identity theft

One of the main reasons companies' fraud prevention strategies fail is they focus on transactions rather than customer identity. Identity theft remains a significant problem faced by fraud teams; Alloy's Annual Compliance Report for 2023 found identity theft was one of the top three indicators of suspicious activity detected by fintech compliance teams this year. In 2024, getting to know as much as possible about customers throughout their lifecycle will help banks understand who is committing fraud or might commit it in the future.

I predict a key investment area will be in enhancing identity theft programs, both at origination and throughout the client lifecycle. Also, expect more investments in authentication tools and strategies. Having the ability to identify a client at onboarding is equally as important as authenticating an existing client during a service transaction.

## On the continued emergence of check and in-branch fraud

Expect check fraud to remain a relevant problem in 2024 along with in-branch fraud. This is a consistent theme we are experiencing now that will continue. During 2024, I predict banks will expand the use of their fraud tools to include omni-channel strategies that require more stringent identity checks during in-branch onboarding and transactions beyond just reviewing an ID.

# Conclusion

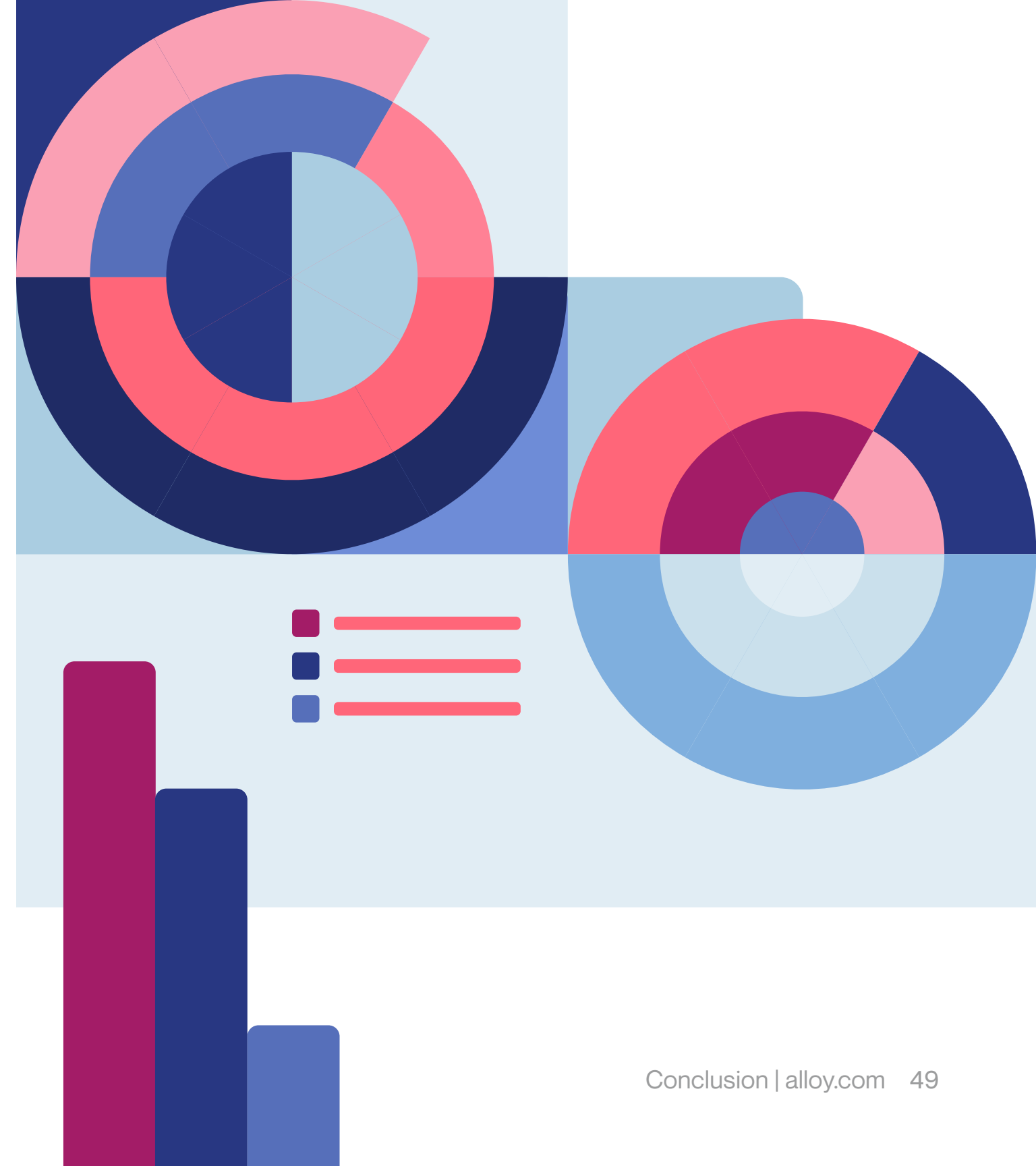


# Conclusion

In 2023, financial institutions (FIs) and fintechs recognized the necessity of investing in more adaptable fraud prevention solutions. But there continues to be a pressing need for broader fraud education to help companies comprehend fraud's intricate nature and steer clear of simplistic remedies — like KBA questions or transaction holds — that add customer friction.

As FIs and fintechs enter 2024, the increasing sophistication of fraud attacks is their foremost concern. This underscores the importance of shifting from transaction-centric to identity-centric fraud prevention models that increase the focus on identifying fraud at onboarding. It is crucial for institutions to remember that there is always a person behind the fraudulent actions, and when they can identify the person, they can stop fraud at a much faster rate.

By focusing on identity, FIs and fintechs will also be able to better identify fraud types and tailor fraud prevention methods to address vulnerabilities and opportunities across different channels. Leveraging third-party fraud solutions and continuous monitoring tools — like Identity Risk Solutions — will enable banks, fintechs, and credit unions to fight fraud more effectively at origination, while they continue to prioritize growth and positive customer experience.



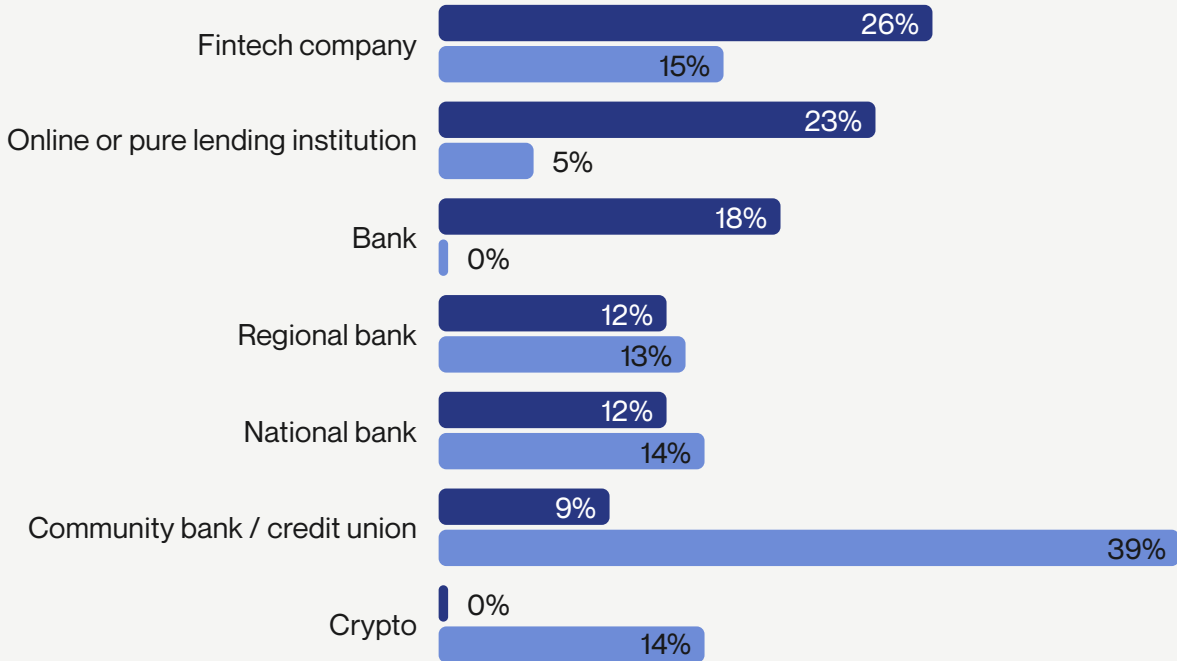
# Appendix

# Changes in survey demographics from 2022 to 2023

2023 2022

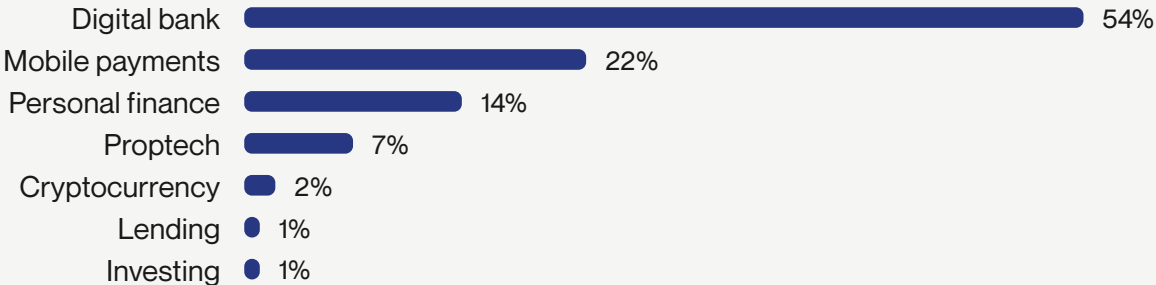
## Company Sector

Bank only asked in 2023, Crypto only asked in 2022

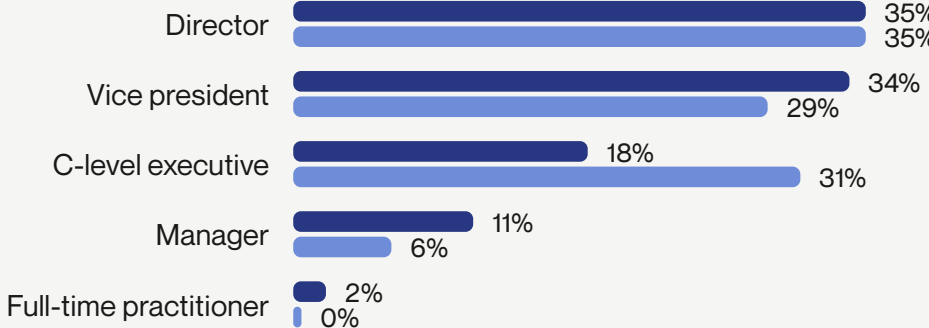


## Fintech company

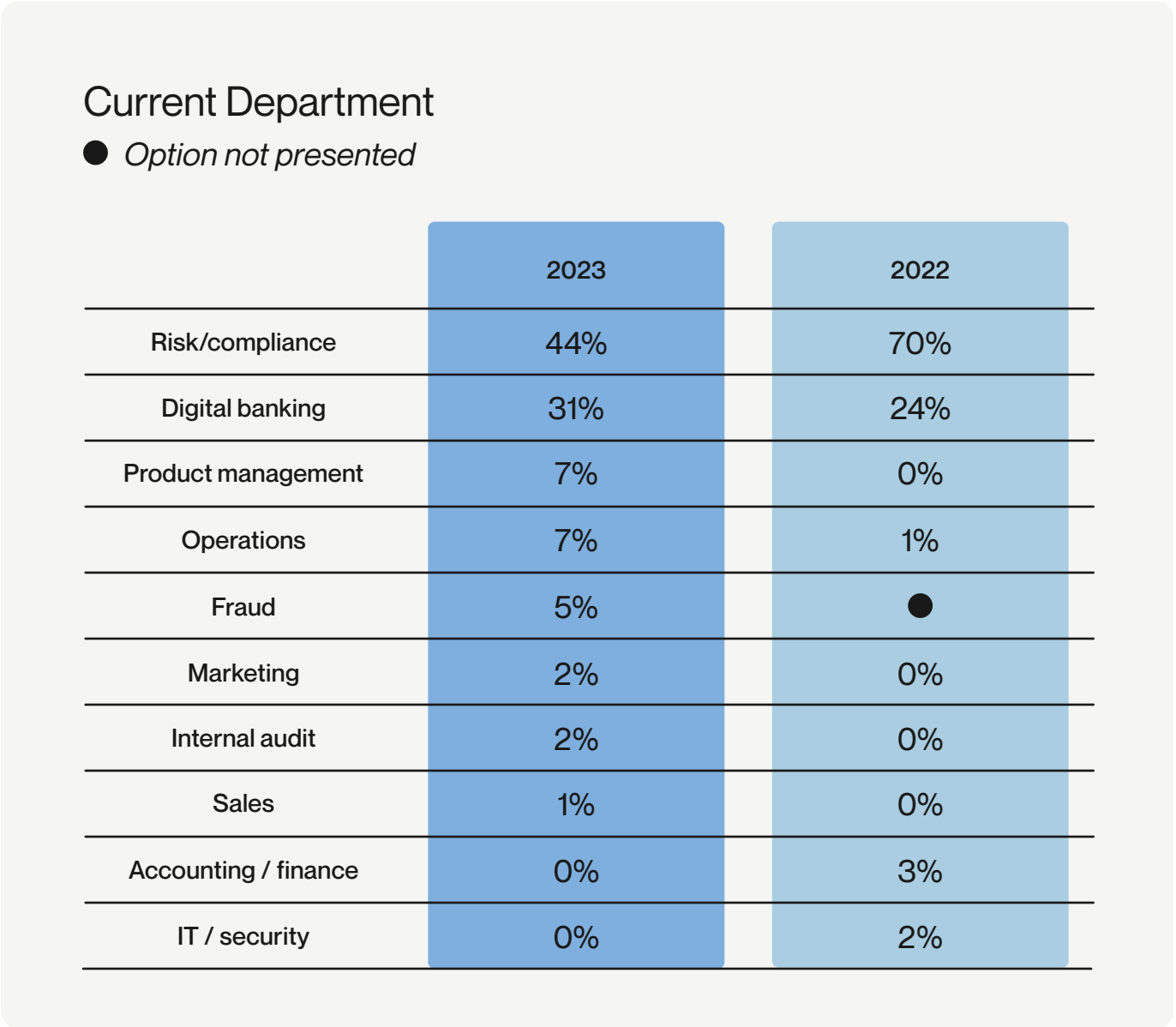
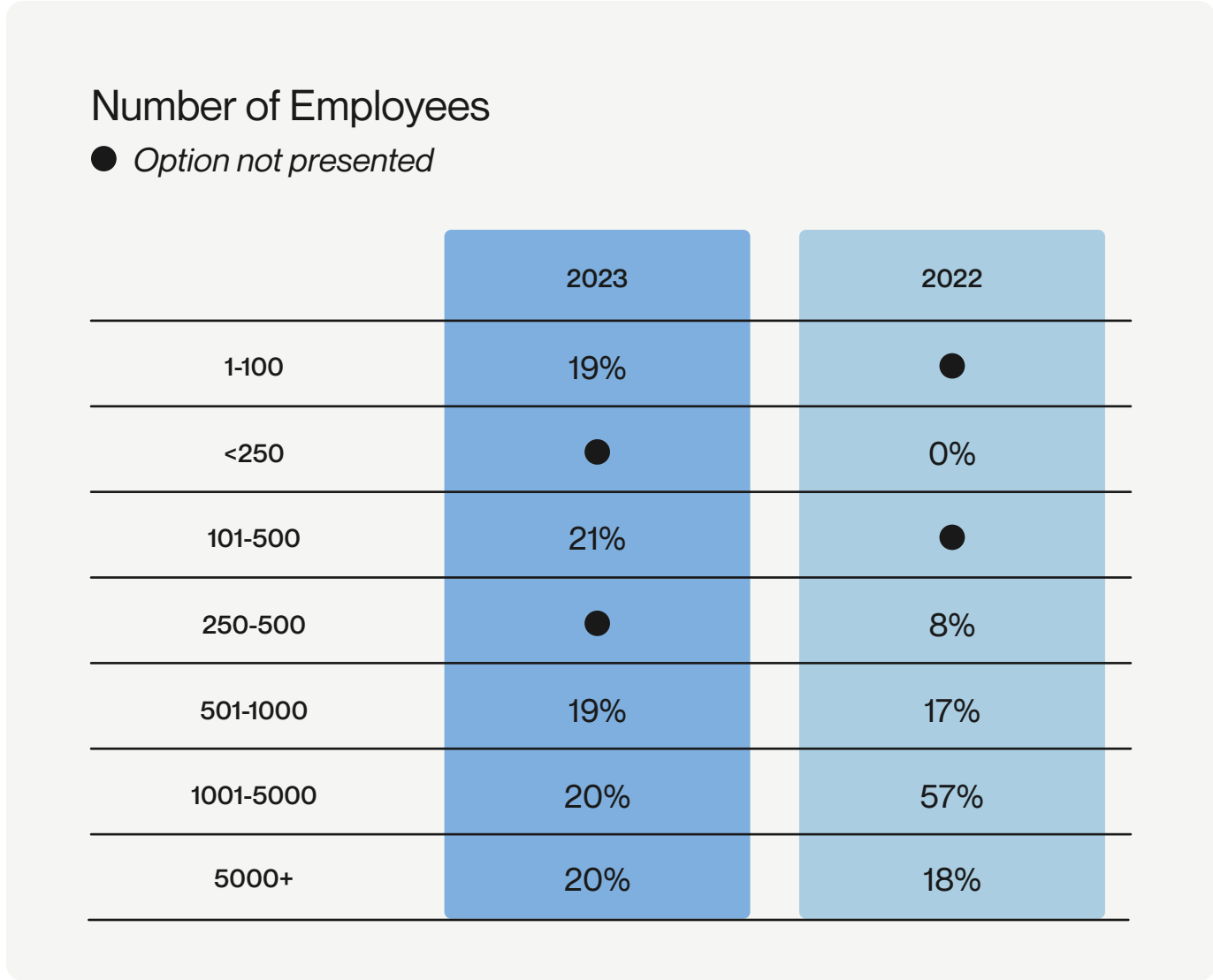
Only asked in 2023



## Job position



# Changes in survey demographics from 2022 to 2023



# About Alloy

Alloy solves the identity risk problem for companies that offer financial products. Today, over 500 banks and fintechs turn to Alloy's end-to-end identity risk management platform to take control of fraud, credit, and compliance risks, and grow with confidence. Founded in 2015, Alloy is powering the delivery of great financial products to more customers around the world.

 [Learn more at alloy.com](https://alloy.com)