ALLOY

2024

UK State of Financial Crime Benchmark Report

Alloy surveyed a total of 450 decision-makers in the UK and the US — 200 in the UK alone — working in fraud-related roles at financial institutions ranging from startup fintech companies to enterprise banks. This report gauges the current state of fraud in the UK.

Generally, the UK exhibited trends that closely matched those of the US. However, there are some distinct nuances in the UK, including:

- Identity theft plays a stronger role in fraud attempts. UK respondents were approximately twice as likely to claim identity theft was the most prevalent form of fraud than US respondents.
- The UK is adding more FTEs to fraud teams as a preventative measure.
- UK respondents were more concerned with AI-driven fraud in the next 12 months than US respondents.

More importantly, UK companies reported slightly greater losses as a result of fraud than the US, and respondents said they were less likely to detect fraud during the onboarding process. However, the majority expressed a growing interest in an Identity Risk Solution, signaling an awareness that fraud prevention at onboarding continues to grow in importance and needs to be addressed.

Table of contents

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***

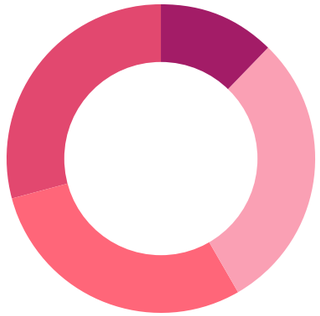
Of the 450 decision-makers:

- **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.

*Includes Building Societies

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 UK and the US

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

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

25%

of companies lost over 1M 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.

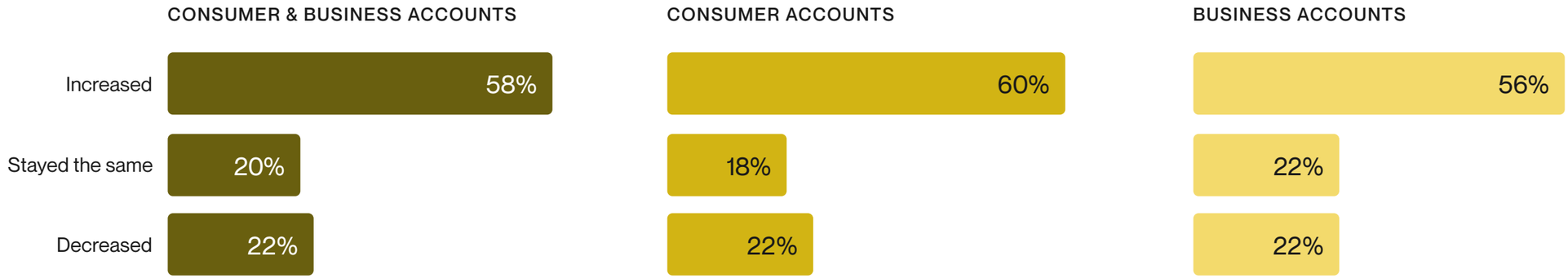
Fraud trends in the UK

Attempted fraud attacks have increased in the last year, especially among consumer accounts.

BENCHMARK

Over half of respondents reportedly experienced an increase in attempted fraud attacks year-over-year.

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



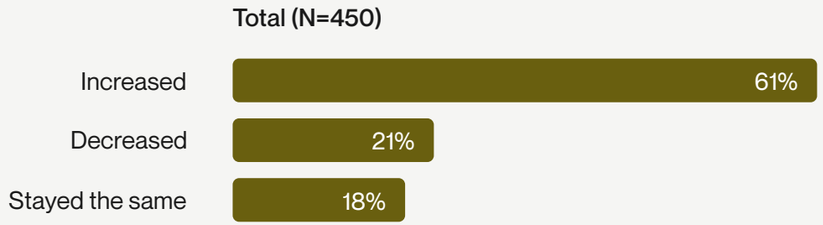
Some sectors saw a decrease in attempted fraud attacks.

Combined UK and US data

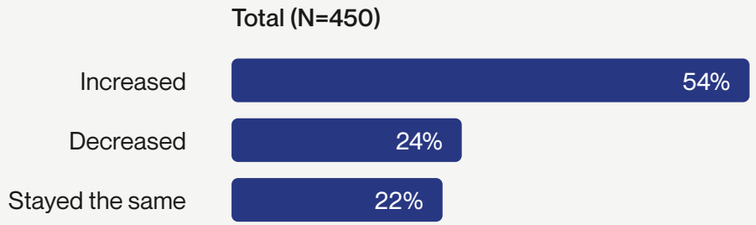
Alloy insight

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%
Increased	73%	66%	52%	61%	46%	36%	63%	57%	54%
Decreased	13%	6%	3%	24%	21%	44%	16%	19%	32%
Stayed the same	13%	25%	45%	15%	34%	20%	21%	21%	14%

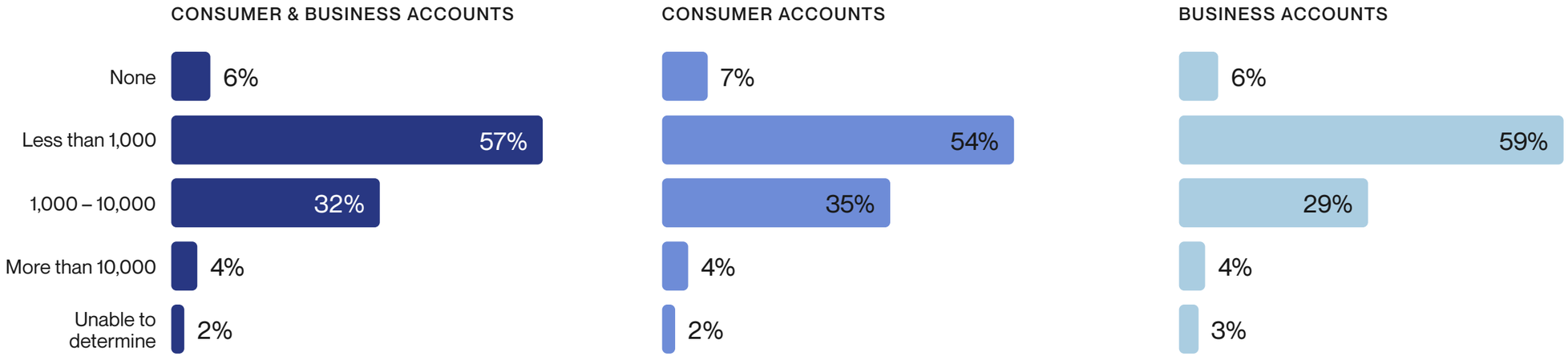
Small base size (<30)

Nearly all UK respondents experienced some level of fraud in 2023.

BENCHMARK

In the UK, 36% experienced 1,000+ fraud attempts in the past year. Respondents reported a slightly higher number of fraud attacks in their consumer accounts — 39% saw over 1,000 fraud attempts in consumer accounts versus 33% saw over 1,000 fraud attempts in business accounts.

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



Manual fraud reviews decreased as a result of fraud prevention tools.

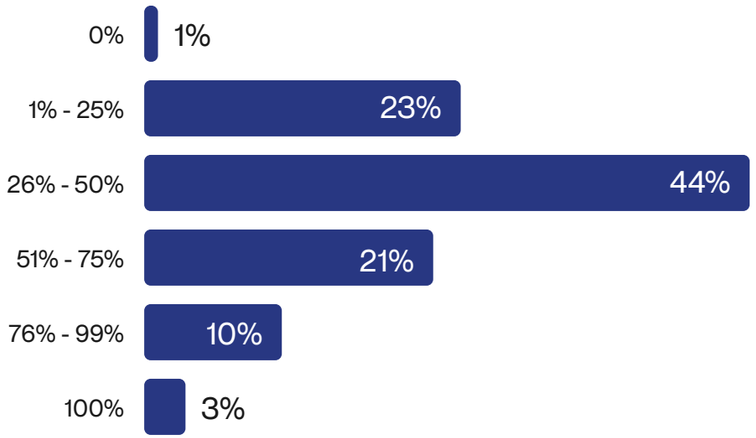
Alloy insight

Manual reviews still occur, but 58% reported that they are less common because of investments in fraud prevention tools.

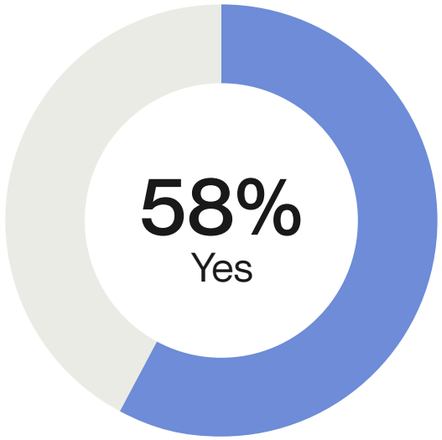
- Among them, 69% observed a reduction of 26%-50% in manual application reviews.

This decrease suggests that when organisations chose to employ these tools, they saw substantial efficiency gains.

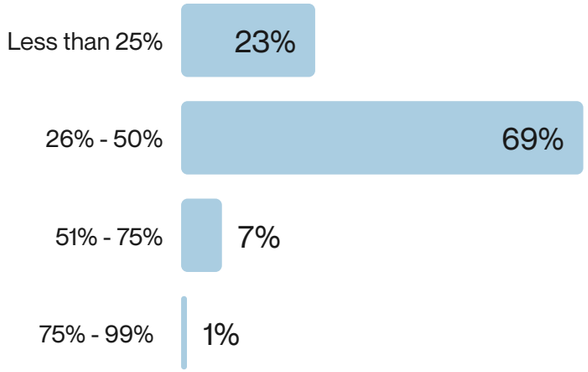
What percentage of new account applications require a manual fraud review by your analysts?



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?



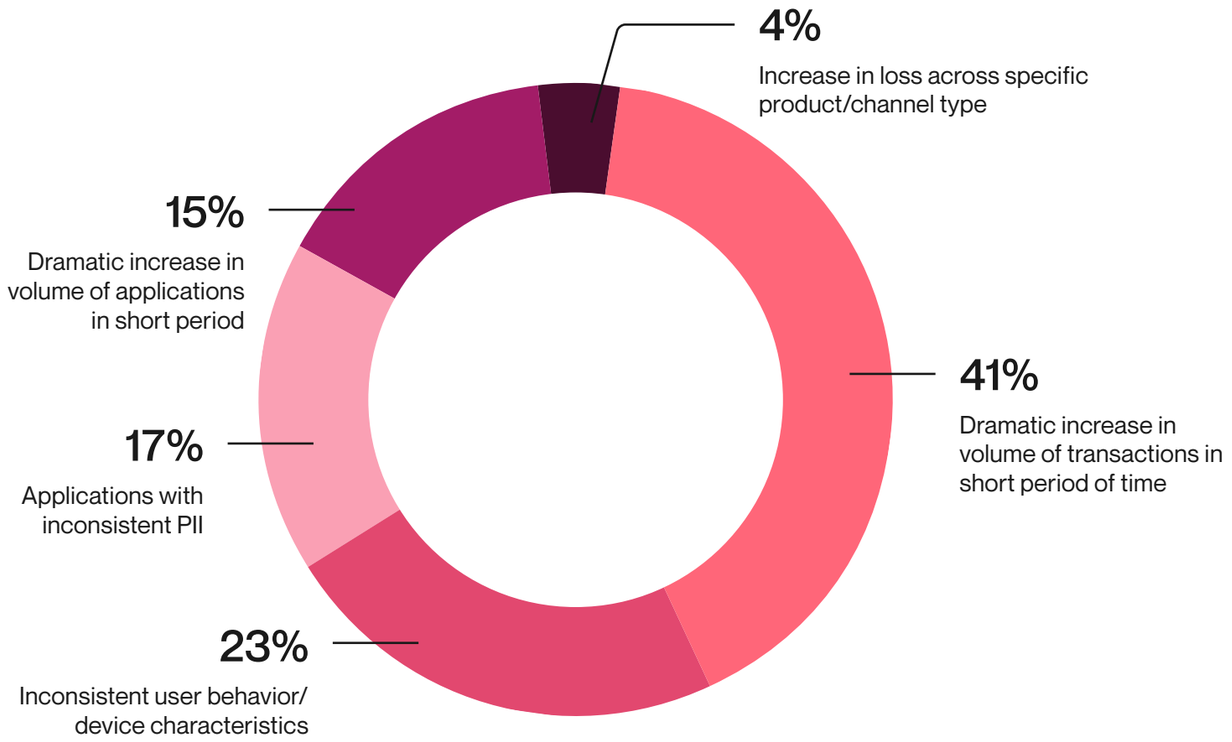
Not shown: 0% (0%), 100% (0%)

How are financial institutions and fintechs catching fraudsters?

BENCHMARK

The most common indicator of fraud in the UK is a sharp rise in the number of transactions over a brief period, followed by applications containing mismatched personally identifiable information (PII).

What's the most common flag when attempted fraud occurs?

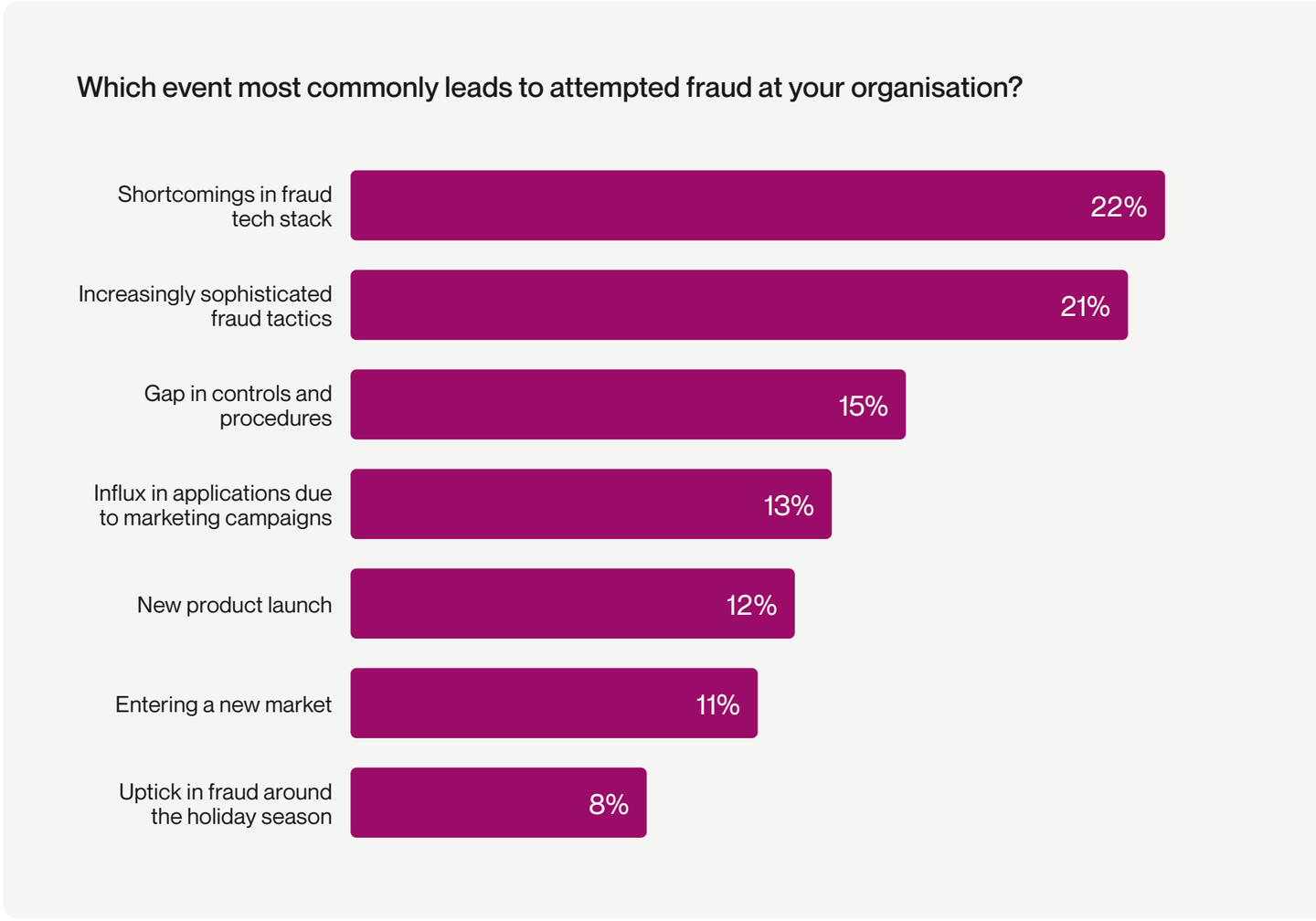


The highest portion of respondents claim that shortcomings in their current tech stack is the most common cause of fraud attempts.

Alloy insight

The largest portion of respondents said that shortcomings in their fraud tech stack and increasingly sophisticated fraud tactics leads to attempted fraud within their organisation.

US comparison: The largest portion of US respondents — **20%** — claimed that increasingly sophisticated fraud tactics are the leading cause of attempted fraud within their organisation. Only **14%** attributed fraud to shortcomings in the fraud tech stack. This could indicate that UK companies are even more in need of third-party fraud prevention solutions than their US counterparts.



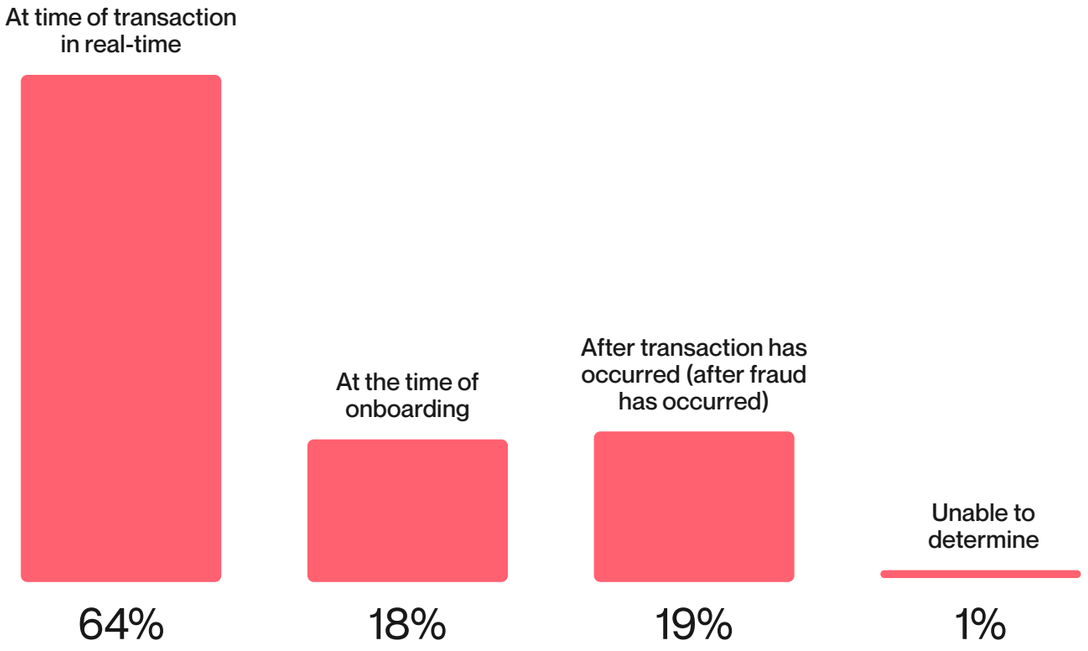
Fraud detection most commonly occurs in real-time.

BENCHMARK

The bulk of UK respondents — **64%** — most commonly detect fraud in real-time at the time of the transaction.

However, **51%** of regional banks reported that they more commonly detect fraud at the time of onboarding.

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

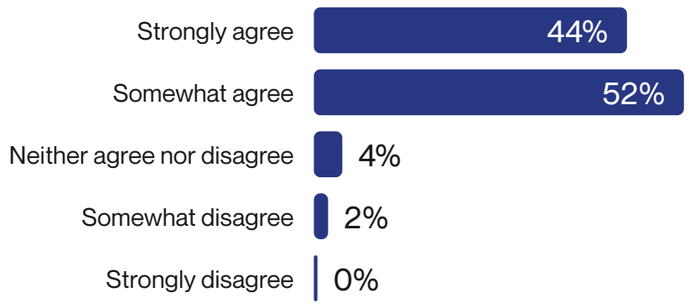


In the UK, two-factor authentication (2FA) is the most common control to prevent fraud before it occurs.

Alloy insight

In the UK, 96% of respondents seem to have confidence in their organisation's ability to manage escalating fraud threats. However, 52% only somewhat agreed, indicating a belief that organisations still have room for improvement in their fraud management practices.

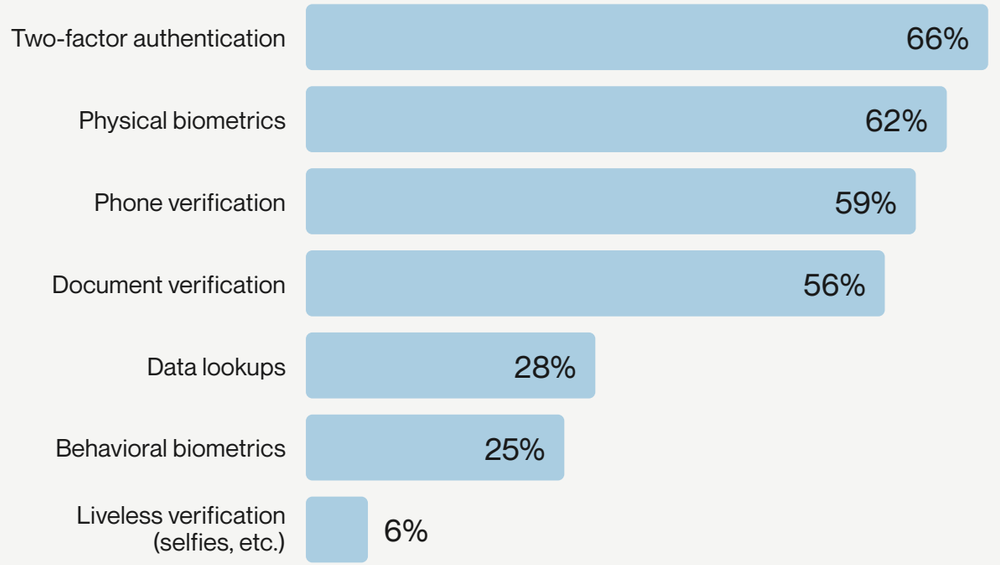
"Our organisation is sufficiently equipped to respond to growing fraud threats."



Alloy insight

UK respondents indicated that physical biometrics are more commonly used than in the US — **62%** compared to **51%**. Meanwhile, phone verification is slightly less common — **59%** versus **61%**.

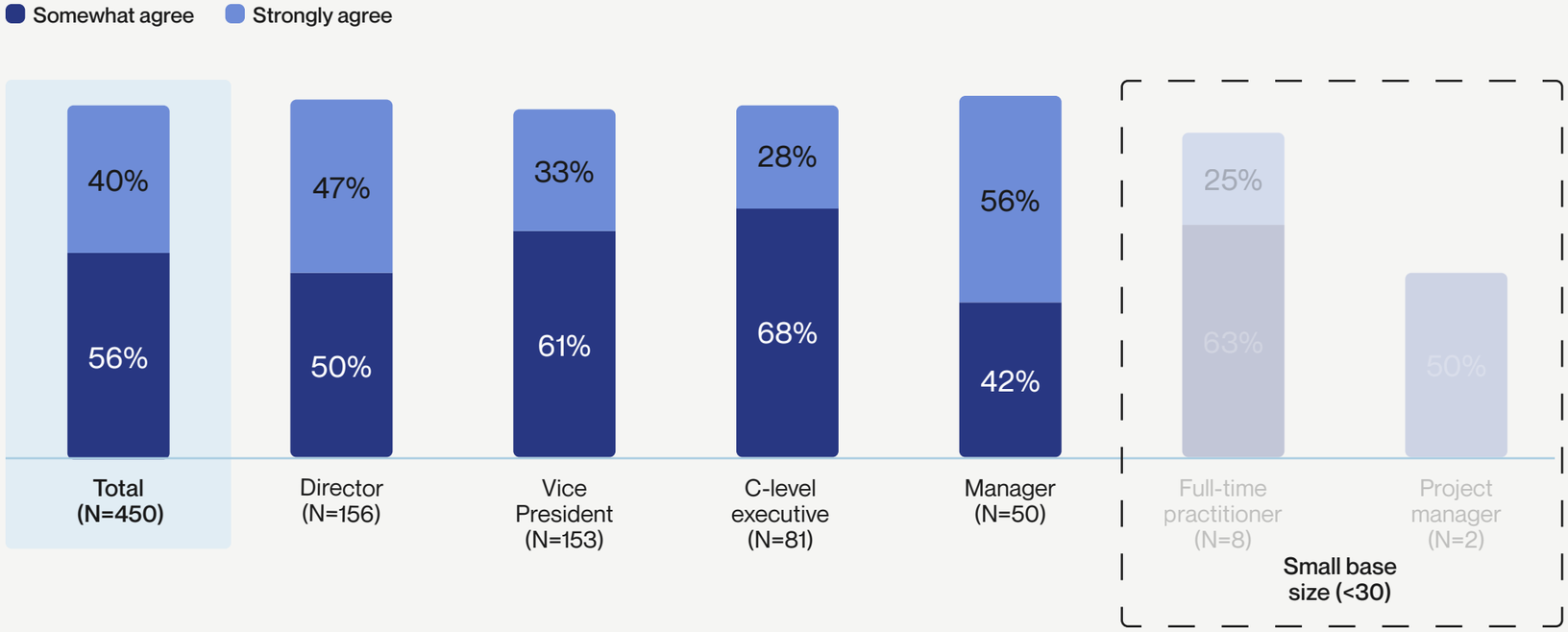
Please select the top three most common controls your organisation uses to prevent fraud.



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

Combined UK and US data

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



Alloy insight

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

Most UK organisations plan to update their existing fraud models.

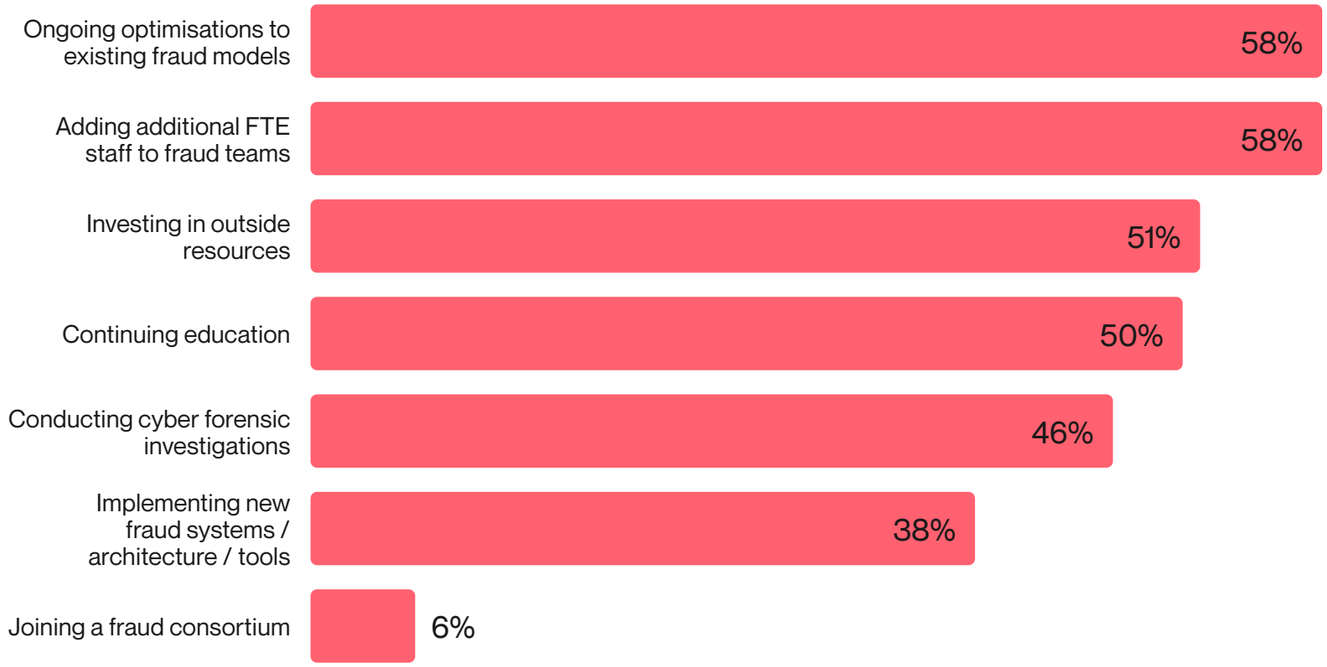
BENCHMARK

Beyond using in-line controls, **58%** said that their organisations are investing efforts in refining their current fraud detection systems and increasing the size of their fraud management personnel.

However, fewer organisations are implementing new fraud systems. This may be causing a drain on resources, since new personnel are focused on fraud instead of building the organisation's core products.

US comparison: In the US, only **43%** of respondents were more likely to add additional full-time employee (FTE) staff to fraud teams, but **48%** were interested in implementing new fraud systems.

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



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

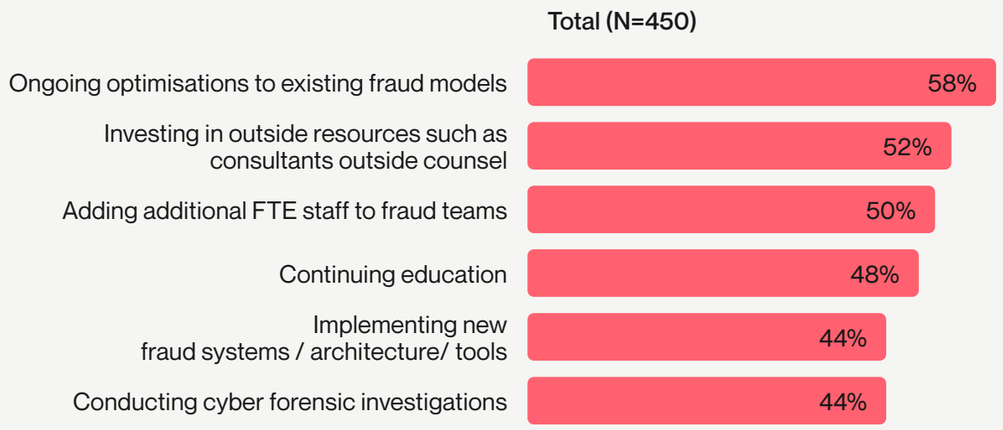
Credit unions (building societies) and community banks are most likely to optimise their existing fraud models.

Combined UK and US 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 8). This might indicate that companies that look beyond just the optimisation 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?



	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)
Ongoing optimisations to existing fraud models	67%	59%	65%	59%	68%	56%	49%	71%	51%
Investing in outside resources such as consultants outside counsel	33%	56%	48%	37%	50%	52%	40%	48%	69%
Adding additional FTE staff to fraud teams	73%	34%	35%	39%	49%	40%	65%	36%	66%
Continuing education	53%	41%	42%	56%	56%	44%	70%	38%	37%
Implementing new fraud systems / architecture/ tools	20%	50%	26%	37%	41%	60%	37%	55%	40%
Conducting cyber forensic investigations	60%	56%	48%	54%	40%	36%	33%	38%	49%

Small base size (<30)

More UK respondents conduct real-time interdiction on transactions as opposed to applications.

Alloy insight

Similar to the US, 96% of UK respondents conduct some form of real-time interdictions.

Approximately 63% of organisations engage in real-time transaction interdiction; roughly half as many — 34% — conduct real-time interdiction on applications.

This indicates a need for stronger investments in fraud prevention solutions that leverage the capabilities of real-time interdiction, so more fraud can be stopped at origination.

63%

conduct real-time interdiction on **transactions**

34%

conduct real-time interdiction on **applications**

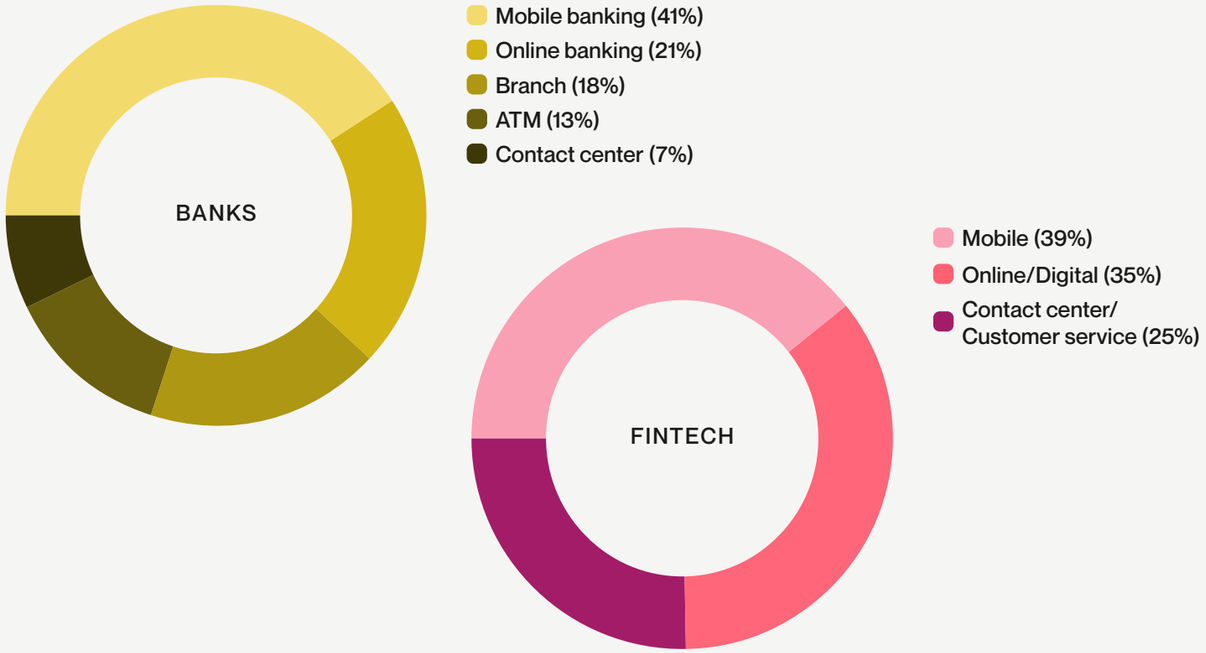
Not shown: No, but plan to (3%), No, not planning on it (1%)

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

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.

Combined UK and US data

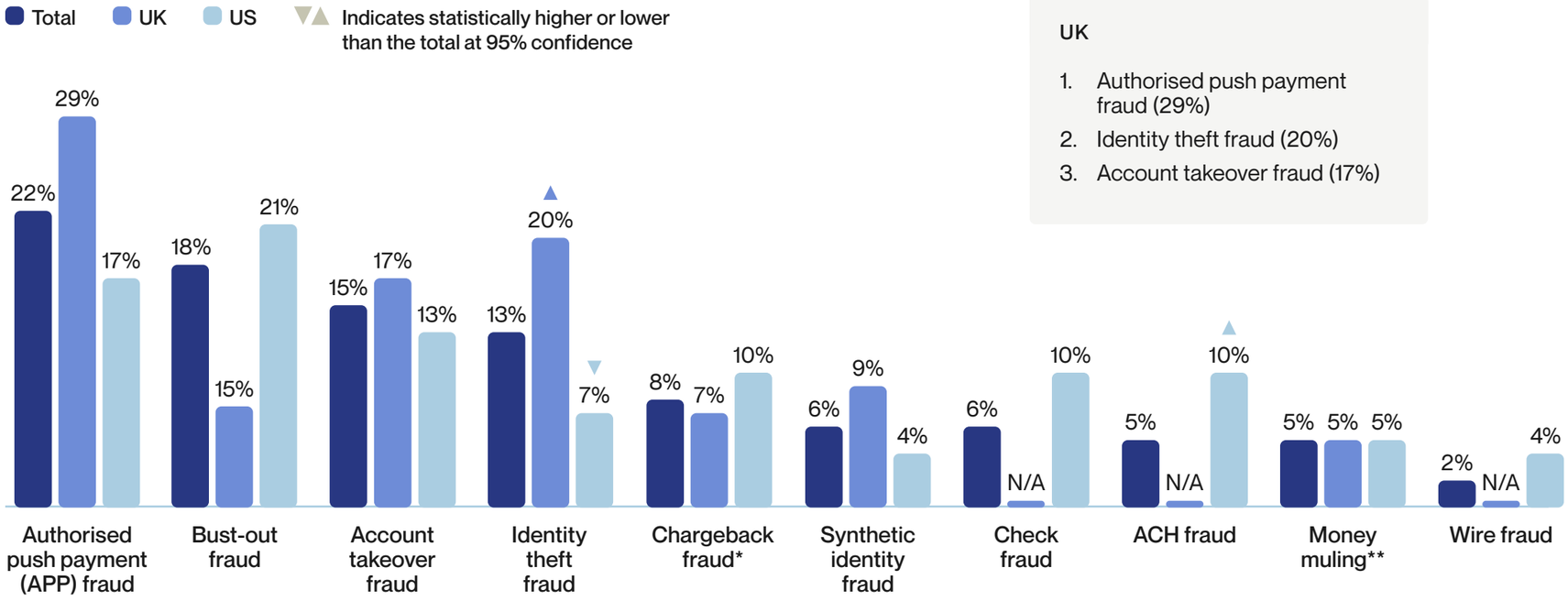
On which channels is fraud most commonly occurred?



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

Combined UK and US data

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



TOP 3

UK

1. Authorised push payment fraud (29%)
2. Identity theft fraud (20%)
3. Account takeover fraud (17%)

*"Friendly fraud" displayed to UK respondents
**"Coercion fraud" displayed to UK respondents

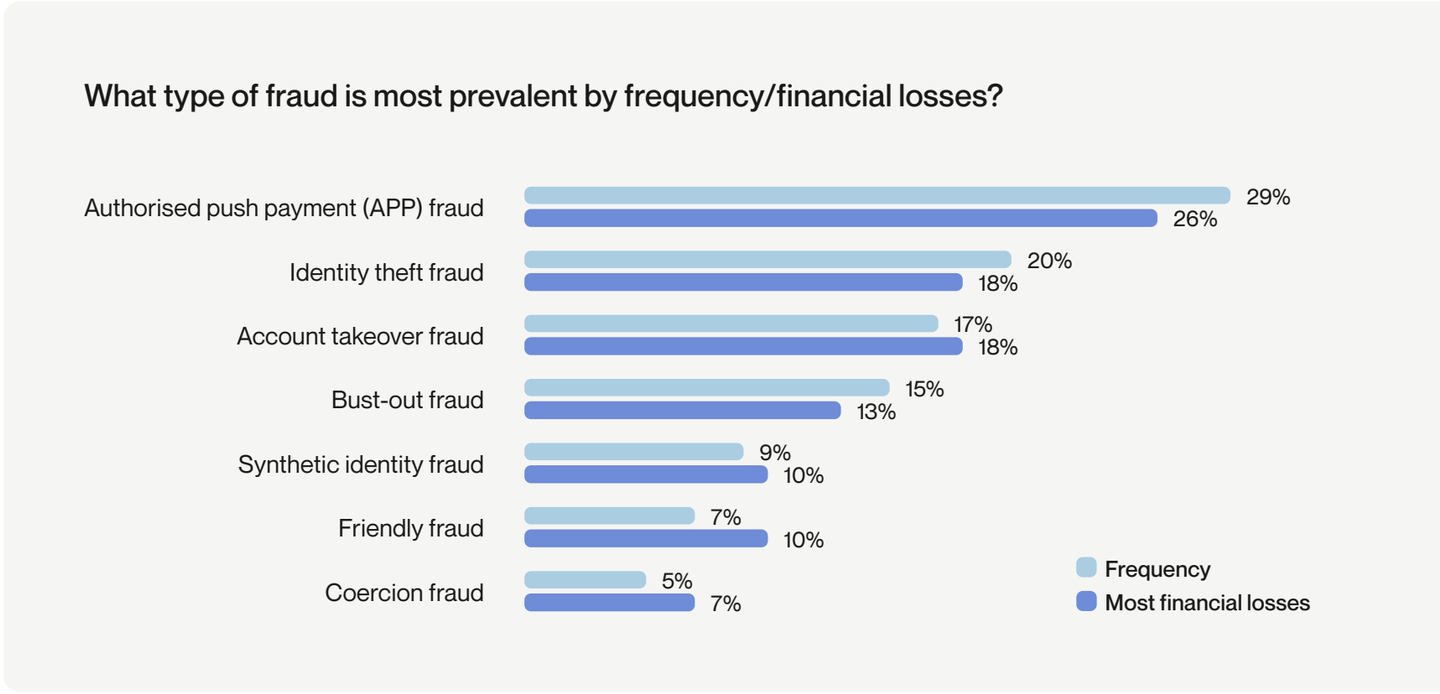
Alloy insight

Authorised push payment (APP) fraud is the most common type of fraud among UK respondents.

Notably, 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%**.

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

APP and identity theft fraud are the most common types of fraud in the UK; they are also the most damaging in terms of financial loss.



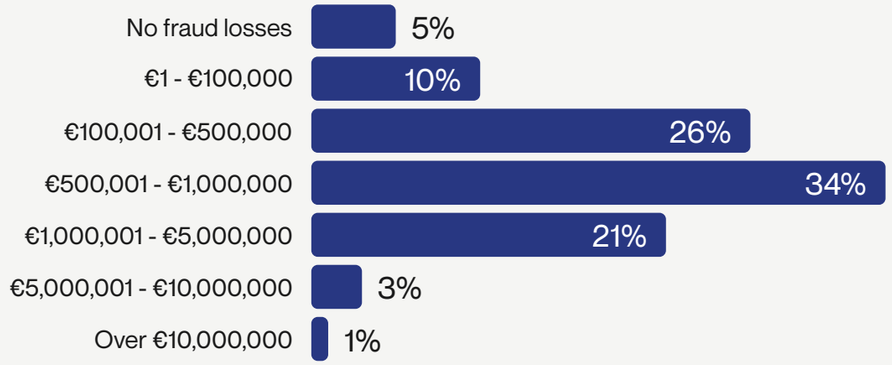
The cost of fraud in the UK

Fraud losses in the UK were high, and respondents were not optimistic about the recovery of fraud losses.

BENCHMARK

Nearly **60%** of UK respondents have lost over €500,000 in the last 12 months; **25%** of that number lost over €1M to fraud in 2023 alone.

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

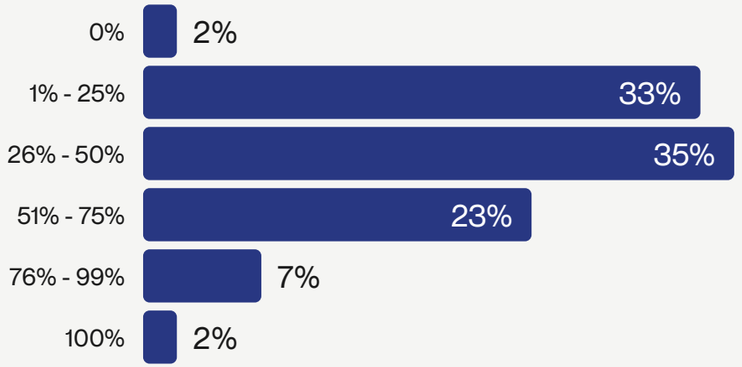


Not shown: Don't know/not sure (2%)

BENCHMARK

On their reported losses, 70% claimed that they were only able to recover 50% or less.

Approximately how much of these fraud losses were recovered?



Direct fraud losses add up faster for smaller organisations

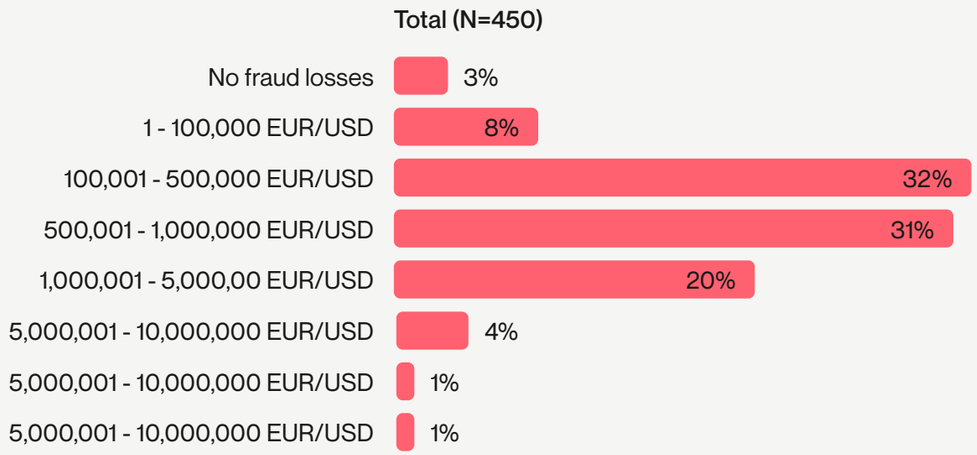
Combined UK and US data

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 (building societies) and mid-market fintechs, which underscores the importance of managing fraud in tightening macroeconomic conditions.

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



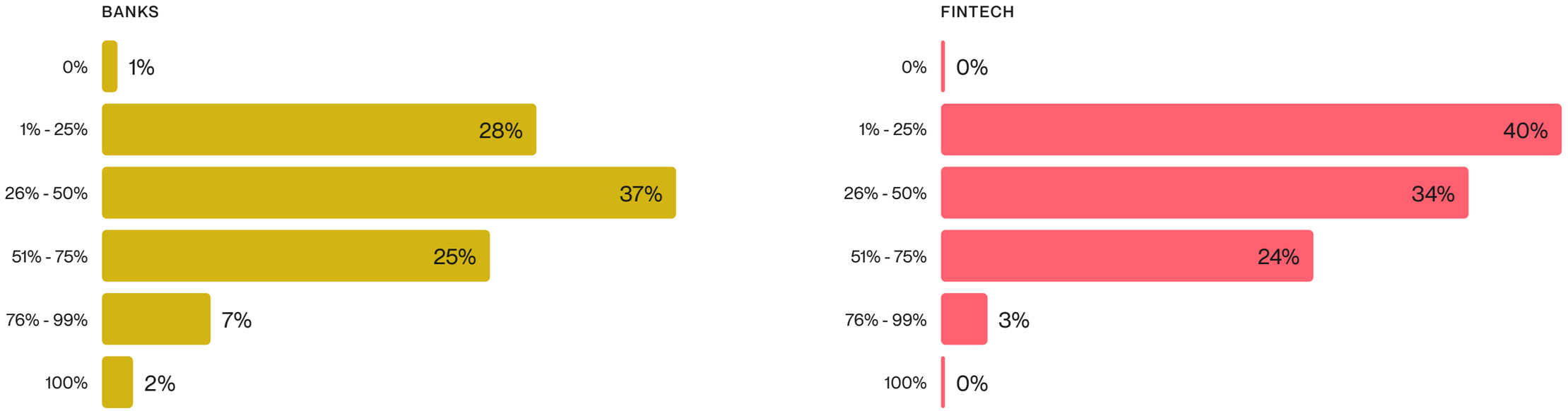
	FINTECH			BANKS				
Growth fintech (N=15)	Strategic fintech (N=32)	Mid-market fintech (N=31)	Enterprise fintech (N=41)	Enterprise bank (N=68)	Mid-market bank (N=50)	Regional bank (N=43)	Credit union/ Community bank (N=42)	Online/ Pure pay lending (N=102)
33%	0%	6%	0%	4%	0%	2%	2%	0%
13%	22%	6%	17%	4%	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%

Small base size (<30)

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

Combined UK and US data

Approximately how much of these fraud losses were recovered?



Loss due to goodwill credit emerged as a big concern in the UK.

BENCHMARK

In the UK, the primary concern for respondents is the direct financial impact caused by fraud. The loss of customers and the threat of regulatory fines ranked lower in comparison. This is consistent with US respondents.

“Loss due to goodwill credit” ended up ranking second overall, which, again, was the same position as the US.

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

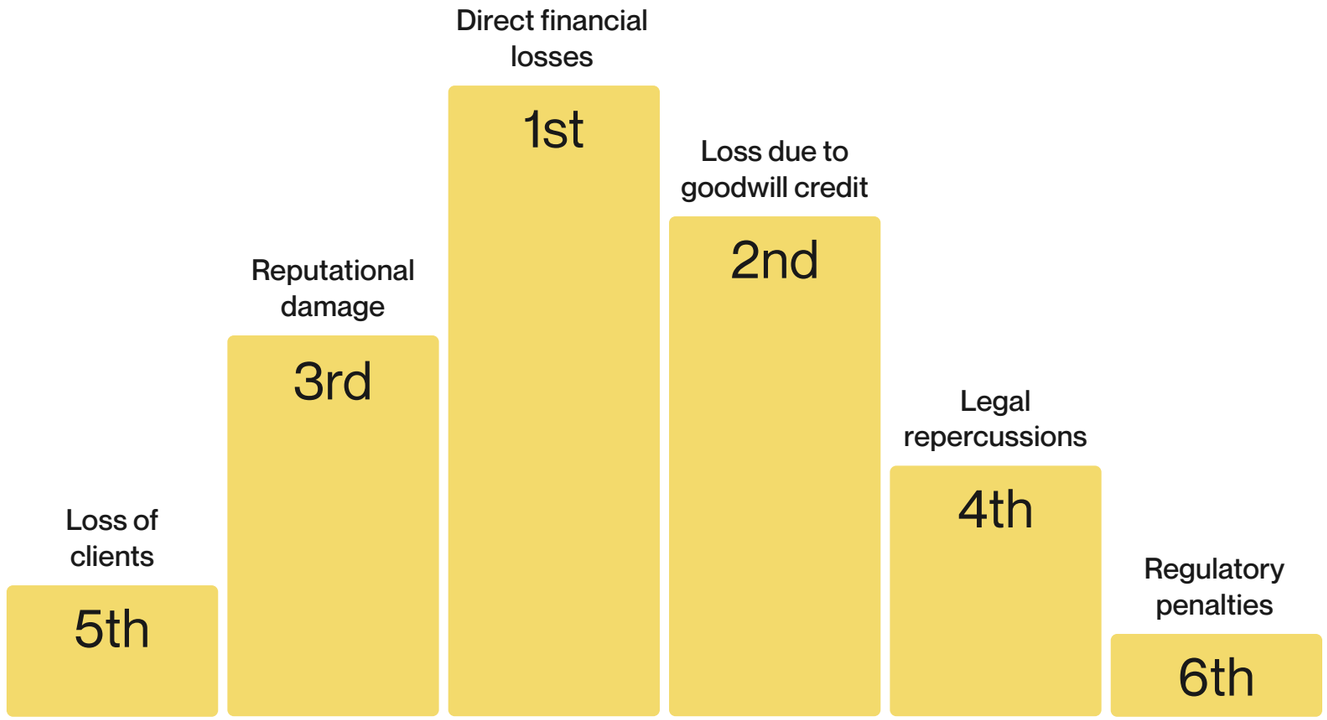


Chart displays choices in order from highest percentage ranked number 1 to lowest

Not all costs are treated equally

Combined UK and US data

Alloy insight

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

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)

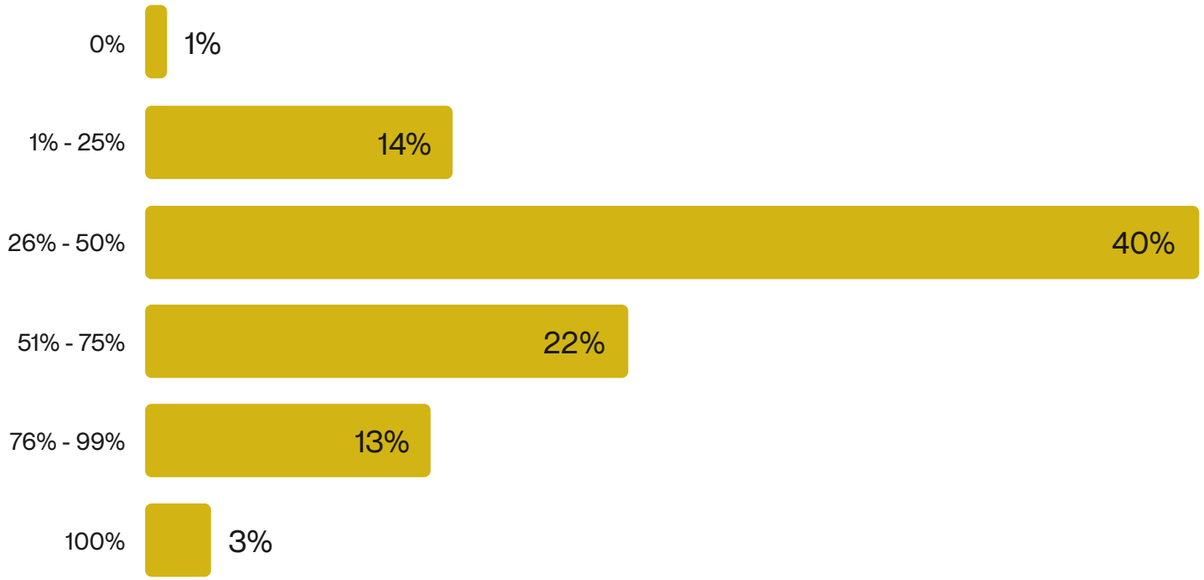
How many developers does it take to solve fraud?

BENCHMARK

In 2023, respondents in the UK did not dedicate the majority of their internal resources to fighting fraud:

- Only 37% of respondents said that more than half of their development teams are focused on fraud-related activities.
- Approximately 63% of respondents said that less than 50% of their development teams are focused on fraud-related activities.

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



UK financial institutions continue to view fraud prevention as a worthwhile investment.

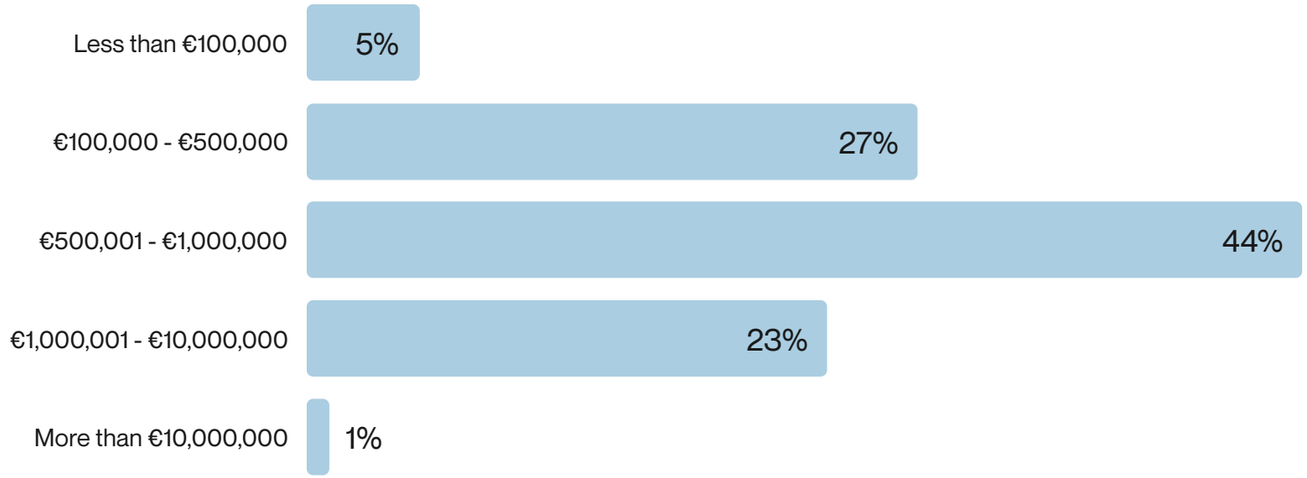
BENCHMARK

The largest portion of respondents spent an estimated €500,000 – €1,000,000 on fraud prevention in the past year. This included investments in their fraud tech stack, labor required to recover and prevent fraud losses, regulatory fines, and goodwill credits to customers.

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

It is important to note that while **59%** of respondents said they lost over €500,000 to fraud, **68%** are also spending over €500,000 on fraud prevention.

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



Not shown: Unable to determine (2%)

Fraud predictions for 2024

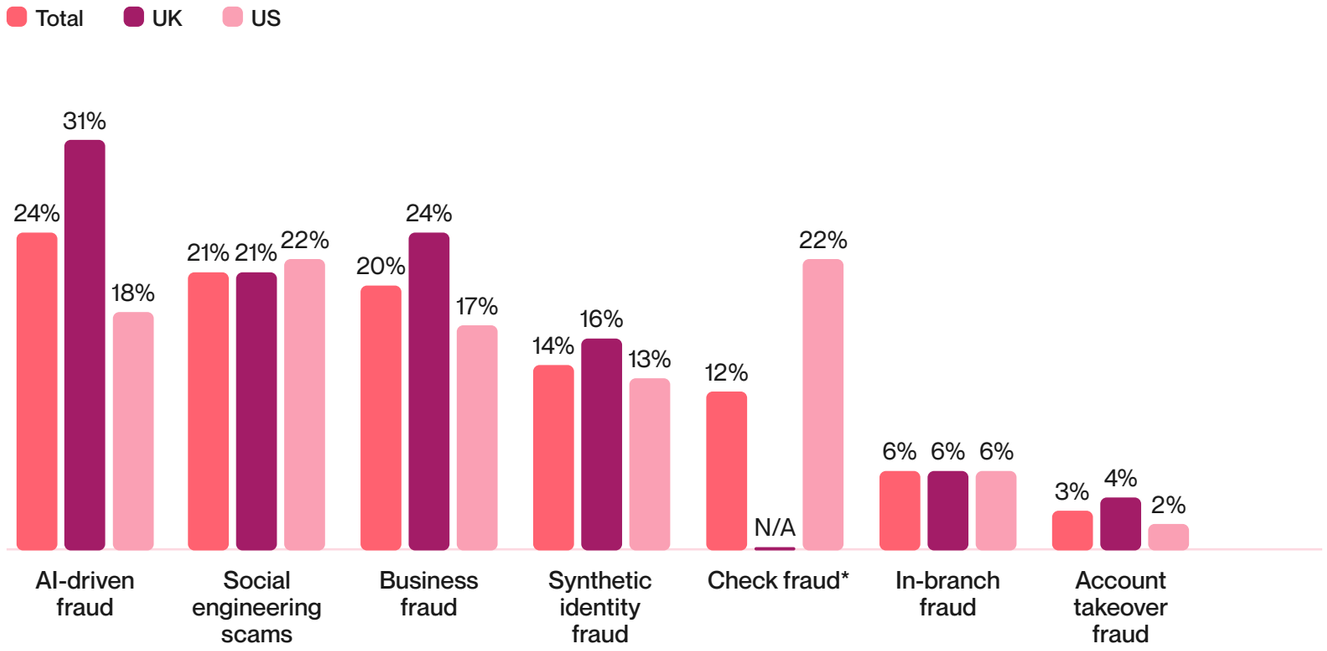
AI-driven fraud and business fraud are UK respondents' primary fraud concerns for 2024.

Combined UK and US data

UK respondents identified their fraud concerns for the coming year:

- UK respondents are more focused on AI-driven fraud, business fraud, synthetic identity fraud, and account takeover 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

Fraud prevention tech investments

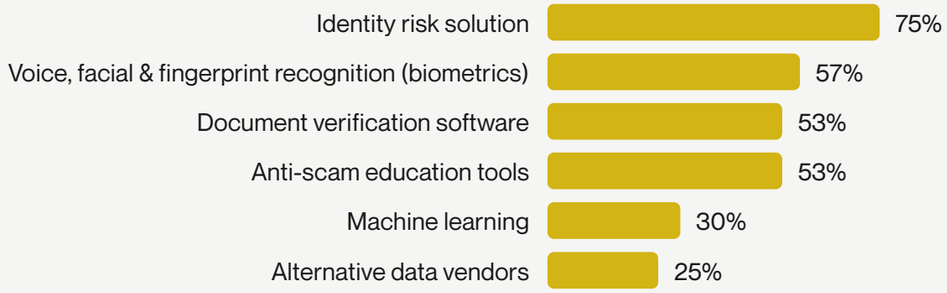
What types of technologies will you be looking to invest in the next 12 months?

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

BENCHMARK

UK and US investments in fraud prevention technology

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

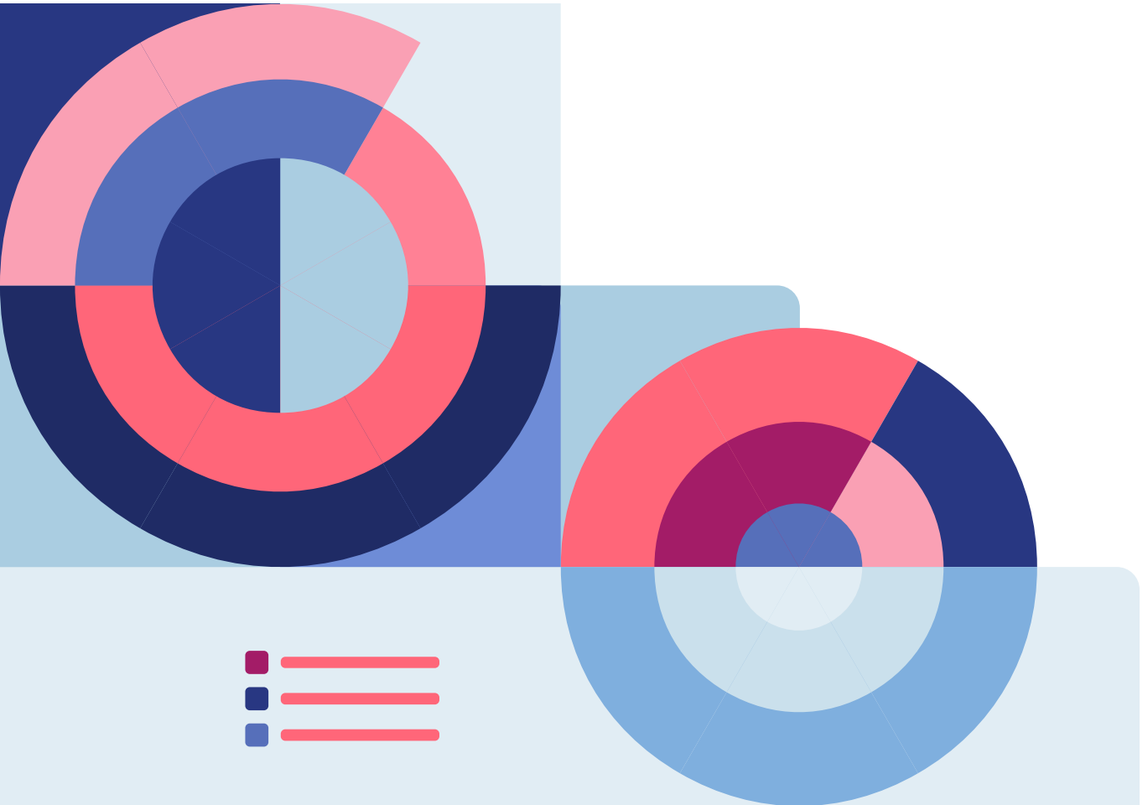


Combined US and UK data

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%

Where will fraud go next in 2024?

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



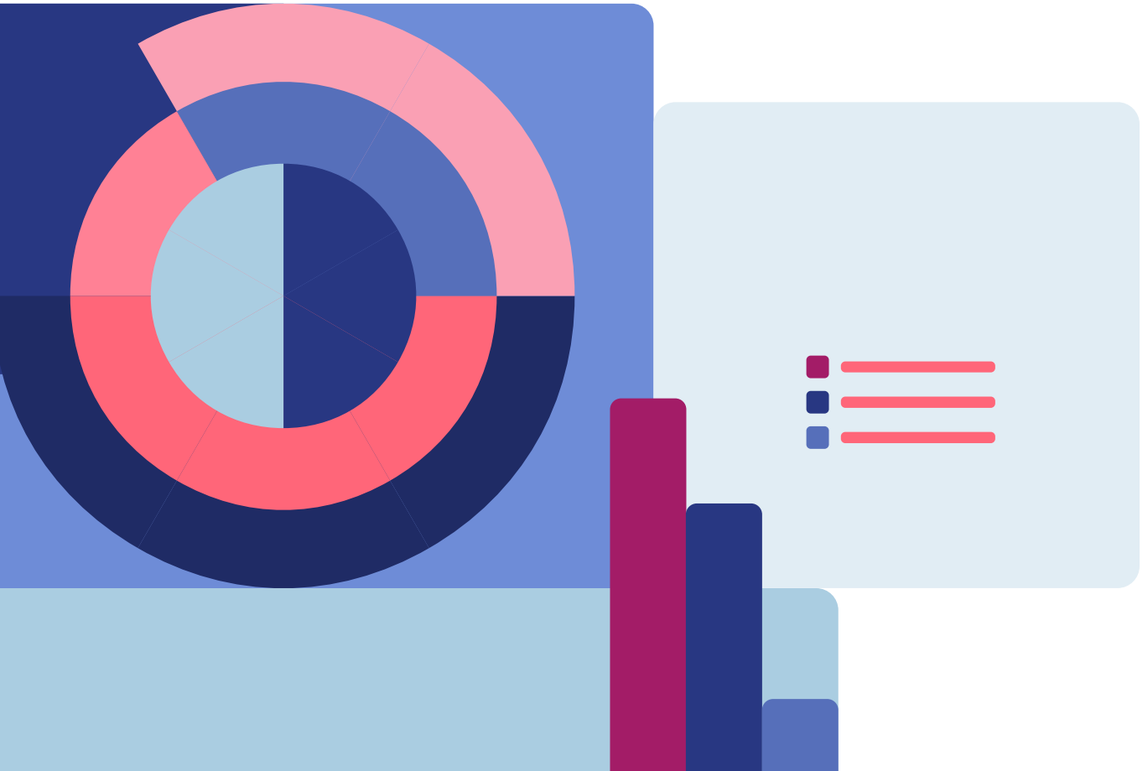
On AI

It's important to note that third-party predictive models have actually utilised 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 behavioural 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 identity theft

One of the main reasons companies' fraud prevention strategies fail is they focus on transactions rather than customer identity. 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 in-branch fraud

Expect in-branch fraud to remain a relevant problem in 2024. 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 omnichannel strategies that require more stringent identity checks during in-branch onboarding and transactions beyond just reviewing an ID.

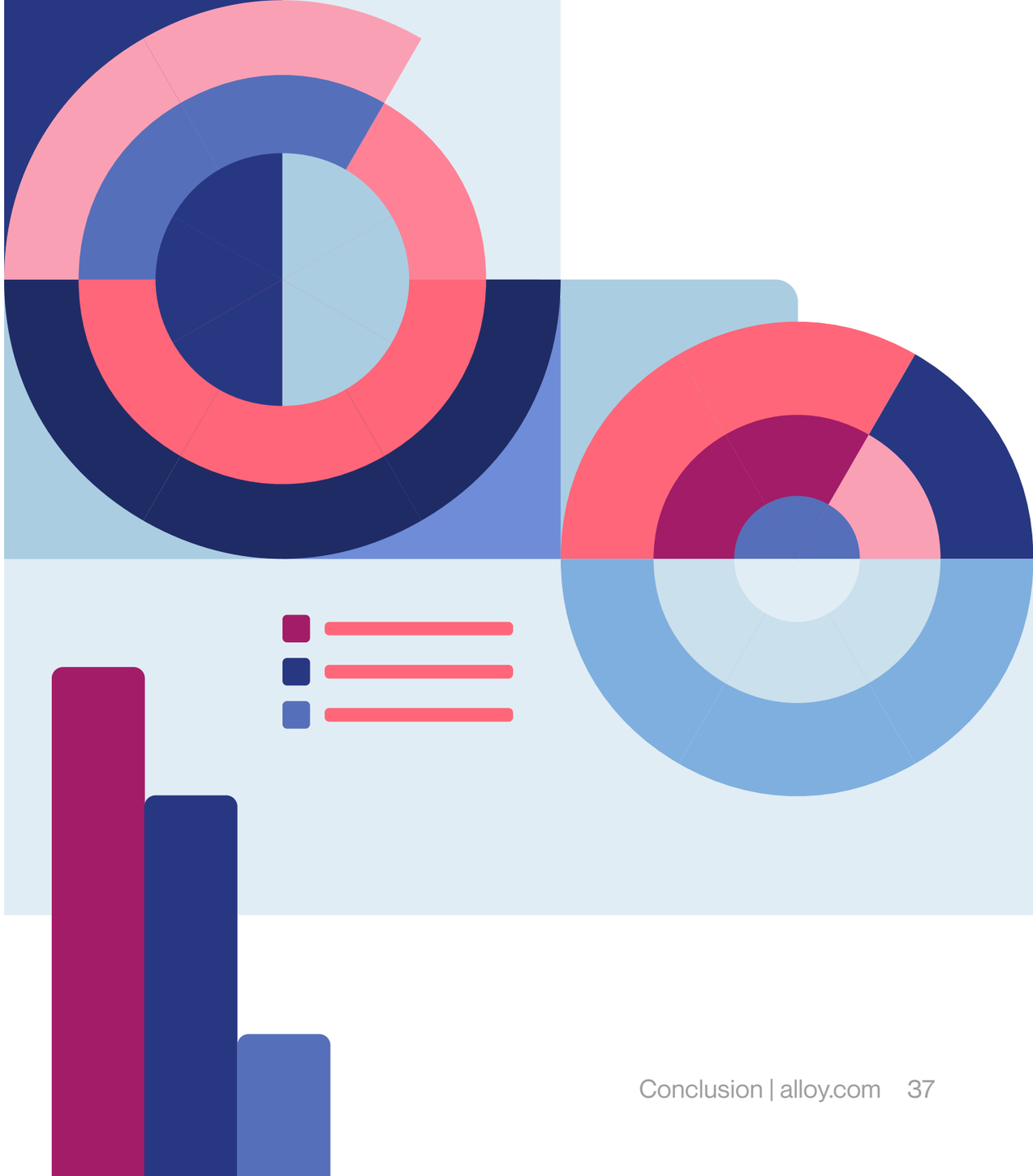
Conclusion

Conclusion

As financial institutions and fintechs enter 2024, the increasing sophistication of fraud attacks is their foremost concern. UK respondents, in particular, were most concerned about AI-driven fraud in the coming year.

This underscores the importance of shifting from transaction-centric to identity-centric fraud prevention models that increase the focus on identifying fraud at onboarding — especially as fraud losses continue to increase and recovery efforts have slowed. It is crucial for organisations 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.

Leveraging third-party fraud solutions and continuous monitoring tools — like Identity Risk Solutions — will enable banks and fintechs to fight fraud more effectively at origination, while they continue to prioritise growth and positive customer experience.



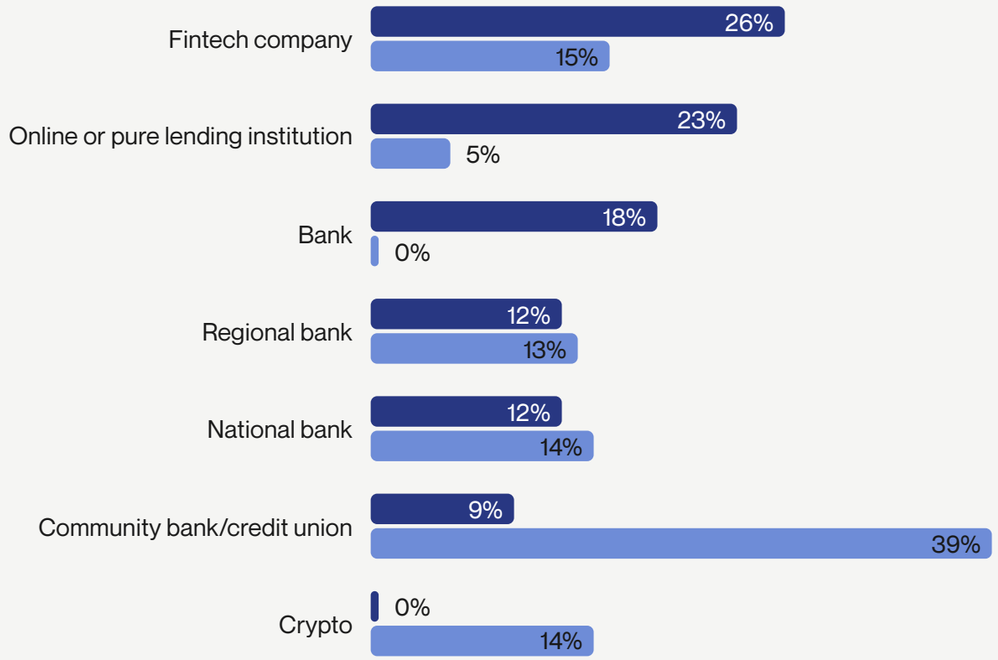
Appendix

Survey demographics

2023 2022*

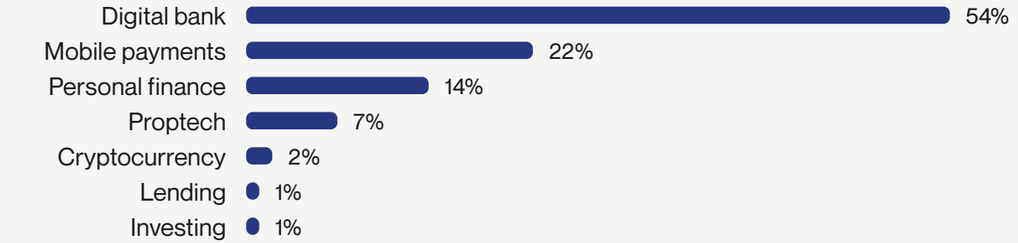
Company Sector

Bank only asked in 2023, Crypto only asked in 2022

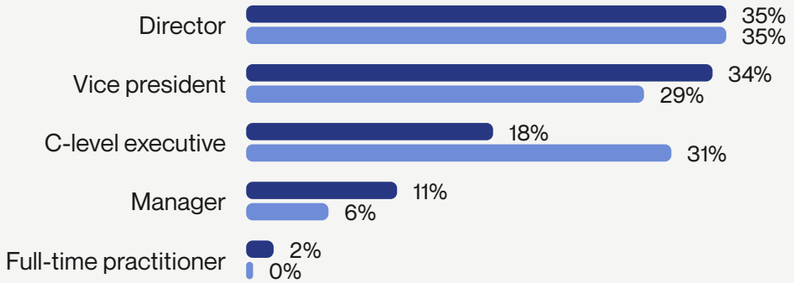


Fintech company

Only asked in 2023



Job position



*The 2022 report surveyed respondents in the US only.

Survey demographics

Number of Employees

● *Option not presented*

	2023	2022
1-100	19%	●
<250	●	0%
101-500	21%	●
250-500	●	8%
501-1000	19%	17%
1001-5000	20%	57%
5000+	20%	18%

Current Department

● *Option not presented*

	2023	2022
Risk/compliance	44%	70%
Digital banking	31%	24%
Product management	7%	0%
Operations	7%	1%
Fraud	5%	●
Marketing	2%	0%
Internal audit	2%	0%
Sales	1%	0%
Accounting / finance	0%	3%
IT / security	0%	2%

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