ALLOY

2025

State of UK Fraud Report

Financial crime trends and predictions, according to UK fintechs

Table of contents

About the survey

About the survey

Methodology

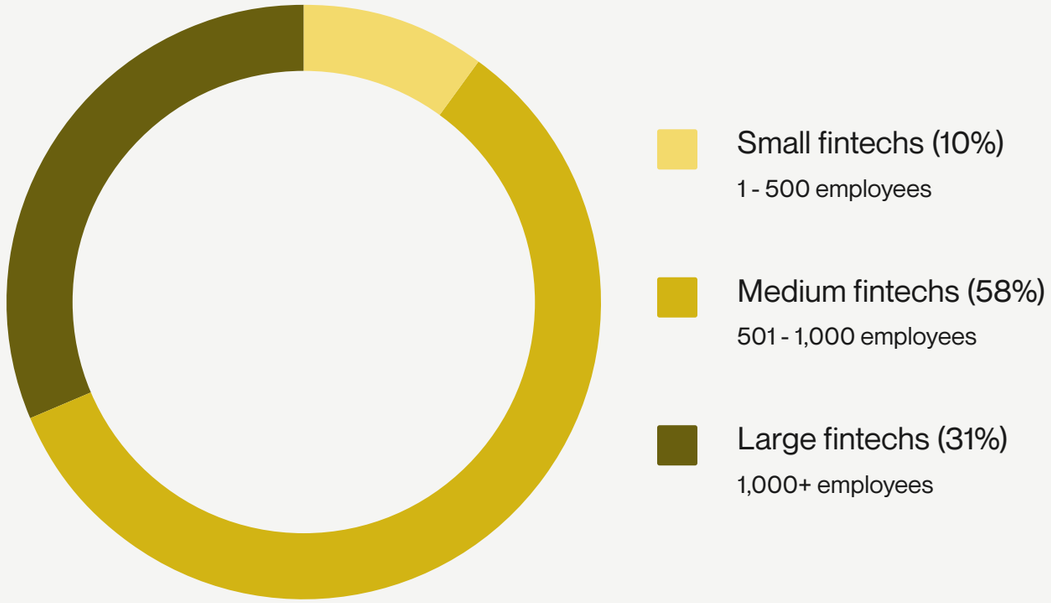
We surveyed **118 industry leaders** at fintechs in the UK.

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

- Risk/compliance
- IT/security
- Fraud
- Operations
- Legal
- Internal Audit

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

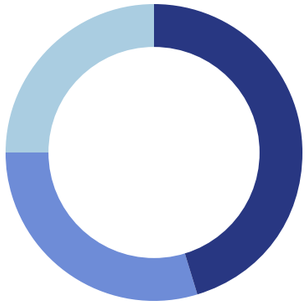
Fintech size by employee count



Demographics

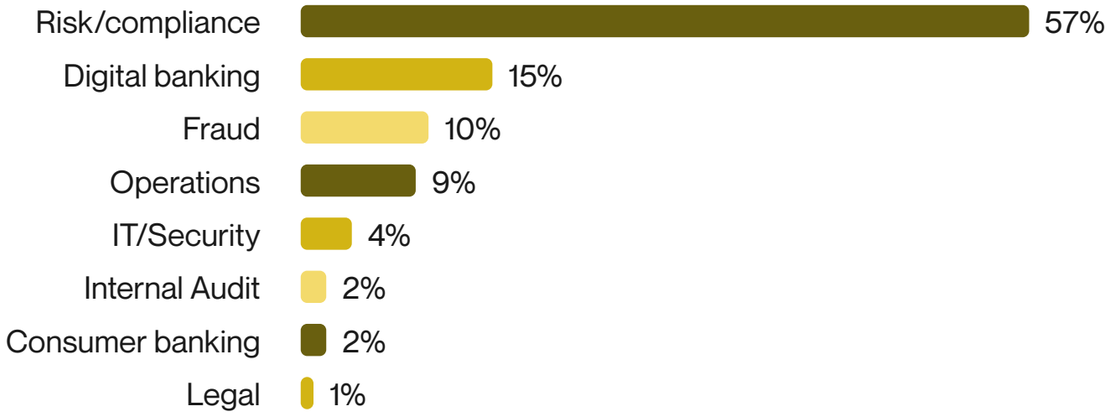
Job position

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



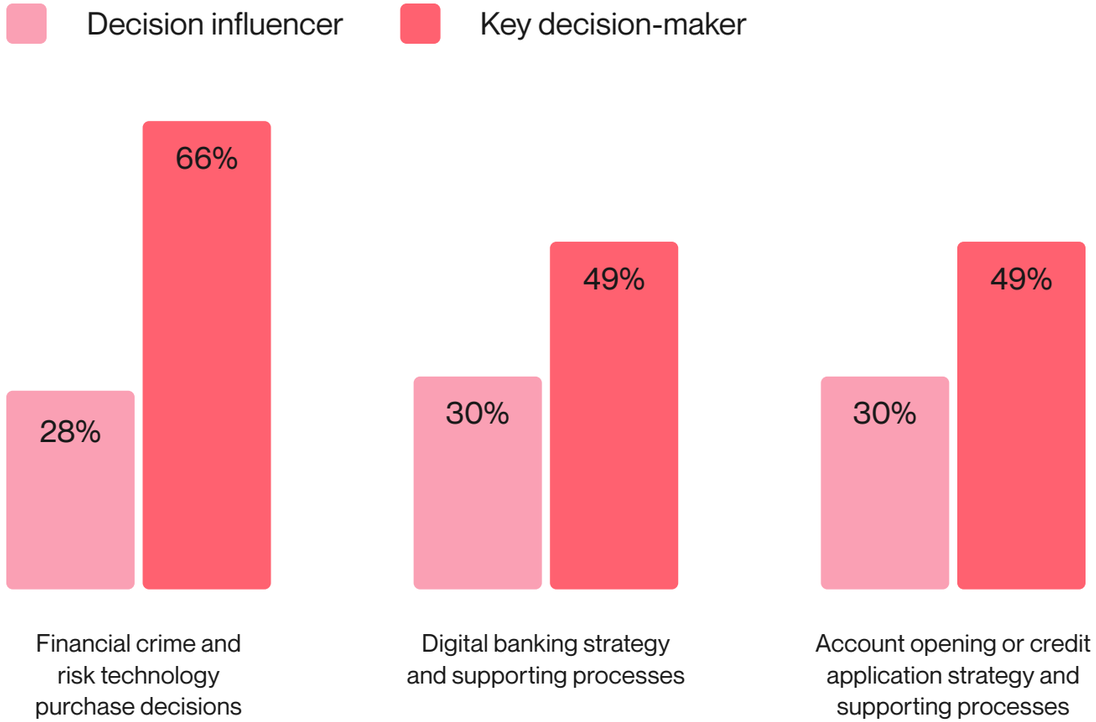
- C-level executive (46%)
- Vice president (30%)
- Director (25%)

Department



Decision-making authority

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



Key findings

UK fraud trends

Industry leaders are focused on meeting regulatory requirements, managing rising fraud losses, and strengthening identity verification as financial crime evolves.

Fraud losses are costly

Fintechs experienced significant fraud losses in 2024.

67%

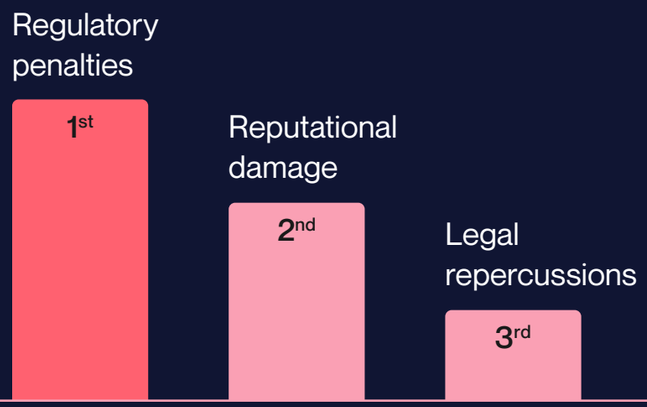
of fintechs reported an **increase in fraud events.**

47%

of fintechs **lost over £1M** to fraud.

Regulatory penalties are a major concern

C-suite leaders ranked regulatory penalties, reputational damage, and legal repercussions as the top three consequences of fraud.



Identity is central to fraud prevention

Leaders are making fraud prevention and technology investments to better understand customer identity and keep up with evolving regulations and fincrime tactics.

38%

named **identity risk solutions** the most impactful fraud reduction investment by their firm in the last 12 months.

72%

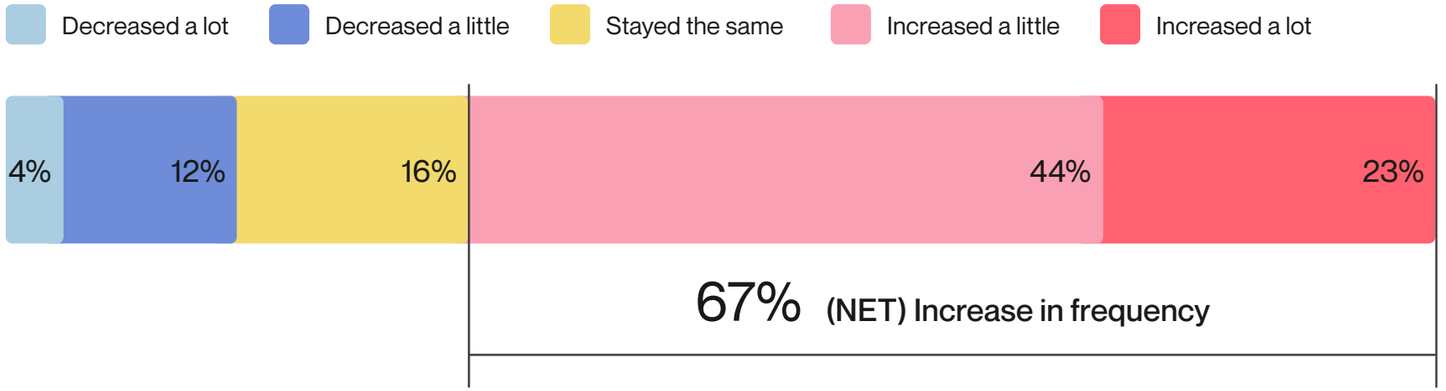
plan to invest in an identity risk solution in 2025.

The fraud landscape

Last year, 67% of UK fintechs witnessed an increase in fraud events.

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

Consumer & business accounts



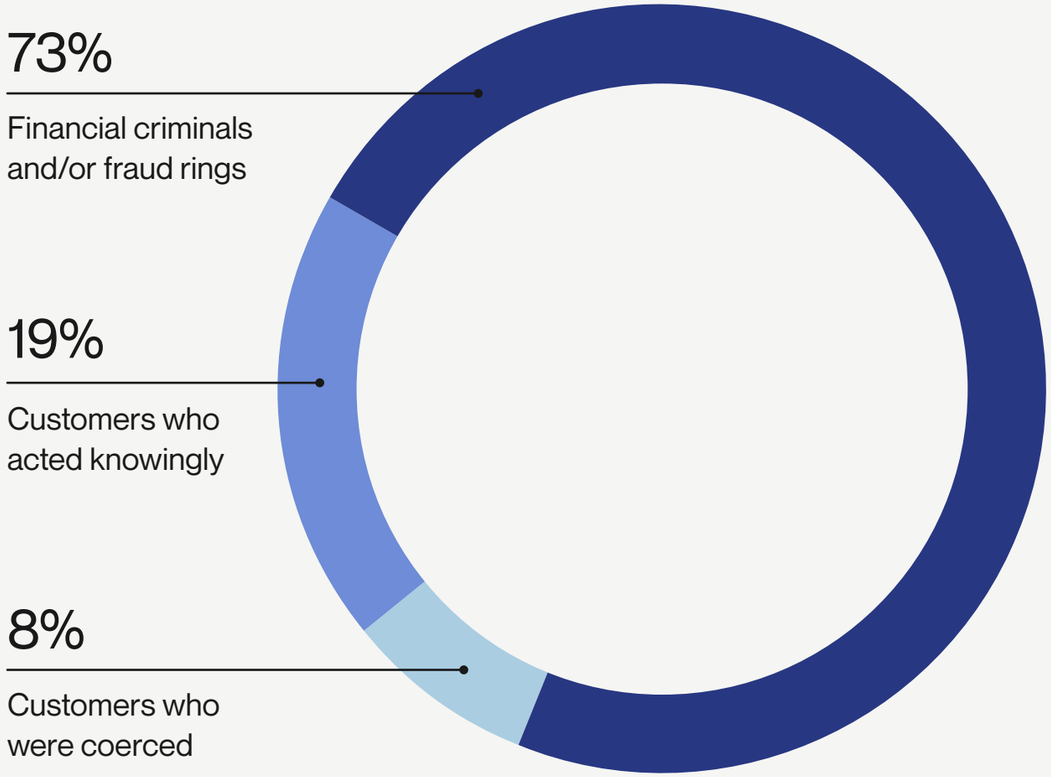
The survey defined a “fraud event” as an effort to exploit a vulnerability in an organisation’s fraud controls and/or the deliberate deception of the organisation, consumer, or business for financial gain.

Respondents overwhelmingly agreed that fraud rings are responsible for the majority of fraud at their organisation.

Alloy insight

A fraudster must weigh the effort of the crime they are committing against the potential reward. AI is reducing that effort and changing that balance in the process. At its core, fraud is a numbers game, and AI is making that game faster, cheaper and easier for crime rings to get right on a global scale.

Who did you determine was responsible for a majority of attempted fraud at your organisation over the last twelve months?



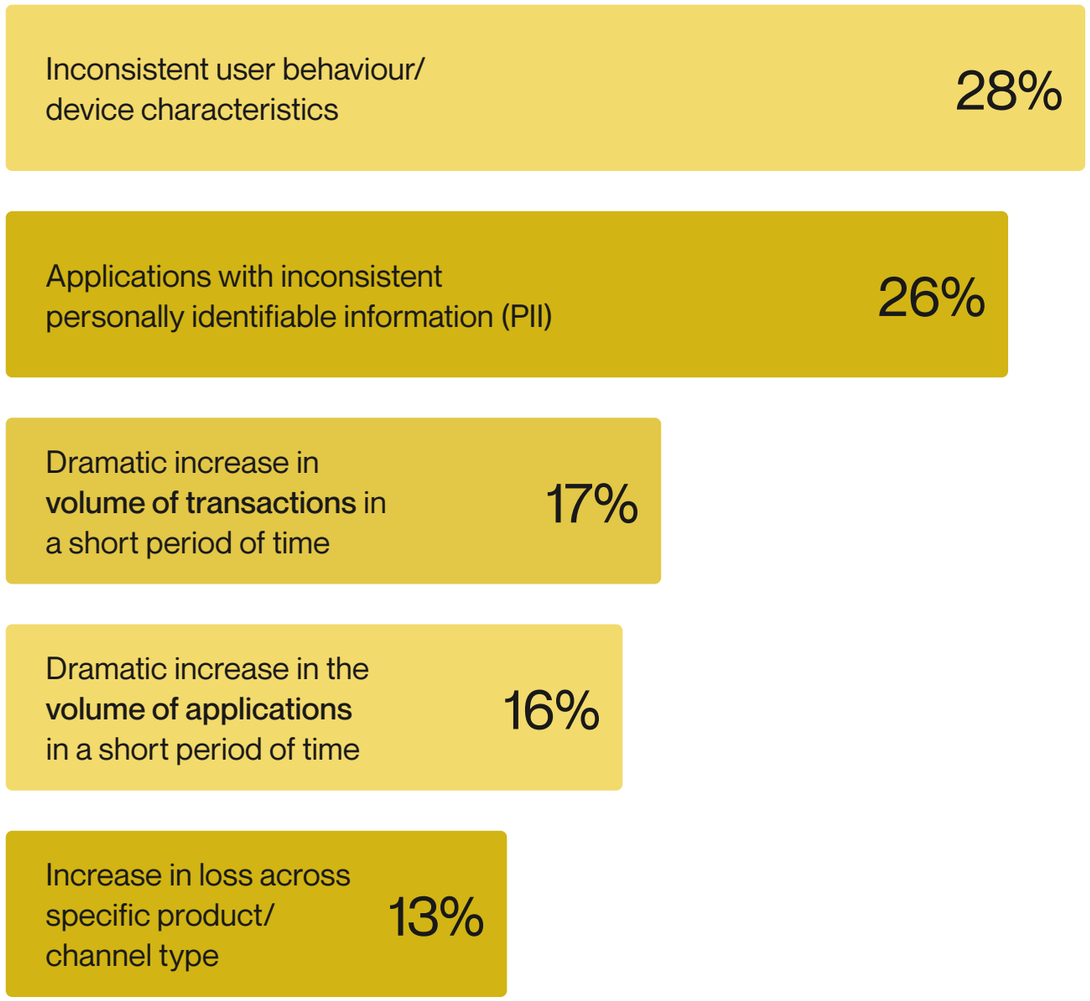
Behaviour, device, and identity inconsistencies were the leading signs of attempted fraud.

Alloy insight

When an account demonstrates inconsistencies in user behaviour or device attributes, such as the type of device accessing the account or the device's geolocation, it points to potential account compromise, as legitimate customers typically maintain consistent patterns in their device usage, login locations, and transaction behaviours.

These anomalies — including sudden changes in IP addresses, unusual login times, or drastic changes in buying patterns — are hallmark indicators of account takeover (ATO) attacks.

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



Insight from

TransUnion

"As organisations continue to digitise, validating the authenticity of a consumer (or potential consumer) becomes critical. Enhancing traditional identity and digital attributes with improved device fingerprinting is one way organisations can stay ahead of bad actors, without introducing unnecessary friction.

Critical to this is ensuring robust underlying data – for example, strong capture rate, returning device recognition strength, and non-human activity detection as well as collecting unique evidence reporting for wider consortia use. A strong data foundation remains key for organisations to leverage flags and predictive models related to device and behavioural insights."

Chad Reimers

TransUnion
General Manager: Fraud & Identity
(UK & Europe)

Fraud costs and consequences

Nearly half of UK fintechs experienced direct fraud losses surpassing £1M.

47% of fintechs incurred **over £1M** in direct fraud losses.

9% of fintechs incurred **over £5M** in direct fraud losses.

Alloy insight

The amount of money lost to fraud by UK fintechs in the UK is comparably higher than that lost by US fintechs, of which only 18% reported losses surpassing $1M (equivalent to approximately £780,000).

The impact of fraud is even more staggering when you consider that direct loss doesn't include expenses such as regulatory fines, money spent recouping funds, and reimbursement costs in the case of APP fraud.

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

Reputational damage, followed by direct fraud losses and legal repercussions, were the most severe consequences of fraud.

Alloy insight

Fraud costs are expanding beyond the financial and cutting across several business areas.

Top fraud consequences negatively impacting UK fintechs

1	Reputational damage	85%
2	Direct financial losses	84%
3	Legal repercussions	84%
4	Regulatory fines/penalties	84%
5	Loss due to goodwill credit to client	81%
6	Loss of clients	79%

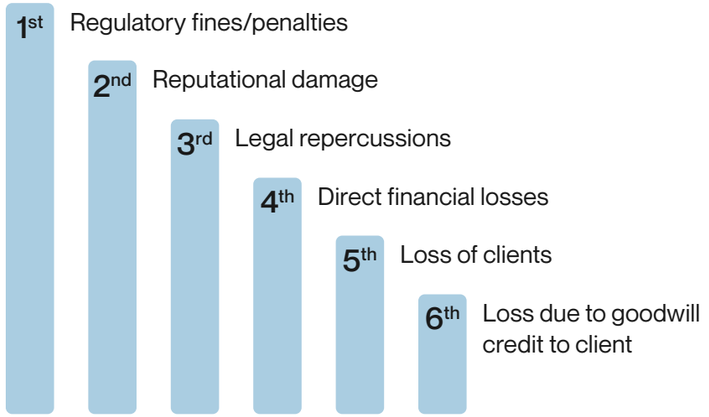
C-suite decision-makers placed a stronger emphasis on regulatory risk and reputational damage than other leaders.

Alloy insight

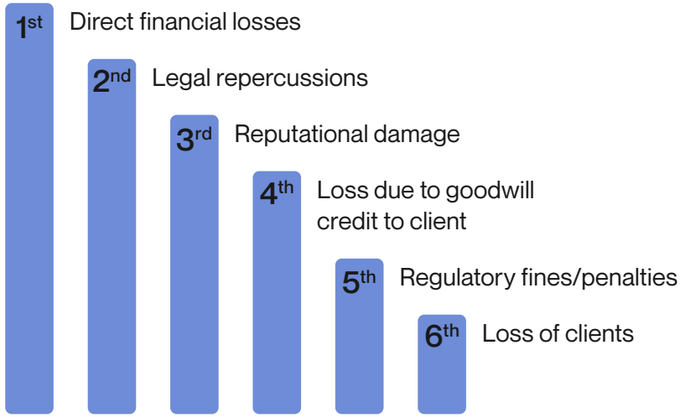
While most C-level executives ranked regulatory penalties and reputational damage as their top concerns, most VPs ranked direct financial losses as their top concern. This discrepancy highlights a divide between strategic and operational risk perspectives: those closer to day-to-day operations appear more focused on immediate financial impacts, whilst C-level leaders concentrate on longer-term strategic risks.

Top fraud consequences by job seniority title

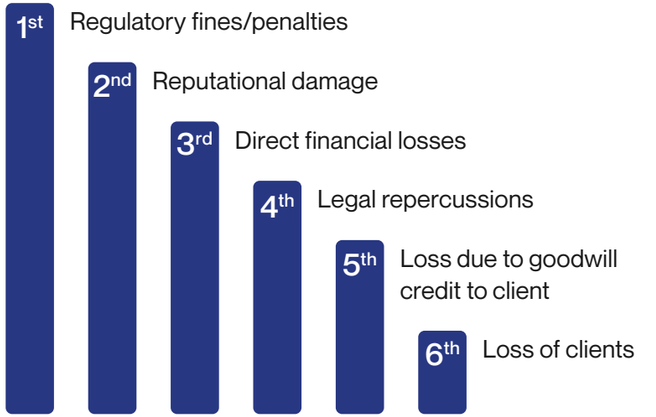
C-Level



Vice president



Director



Insight from

IG Group

Ellen Rogers

Head of Financial Crime Compliance

"As a fast-growing business, meeting compliance requirements is critical for our team when it comes to building trust with both regulators and customers. As a result, we invest a great deal of time and resources into building financial crime prevention policies that stand the test of time with the goal of growing our business without opening ourselves up to additional risk."

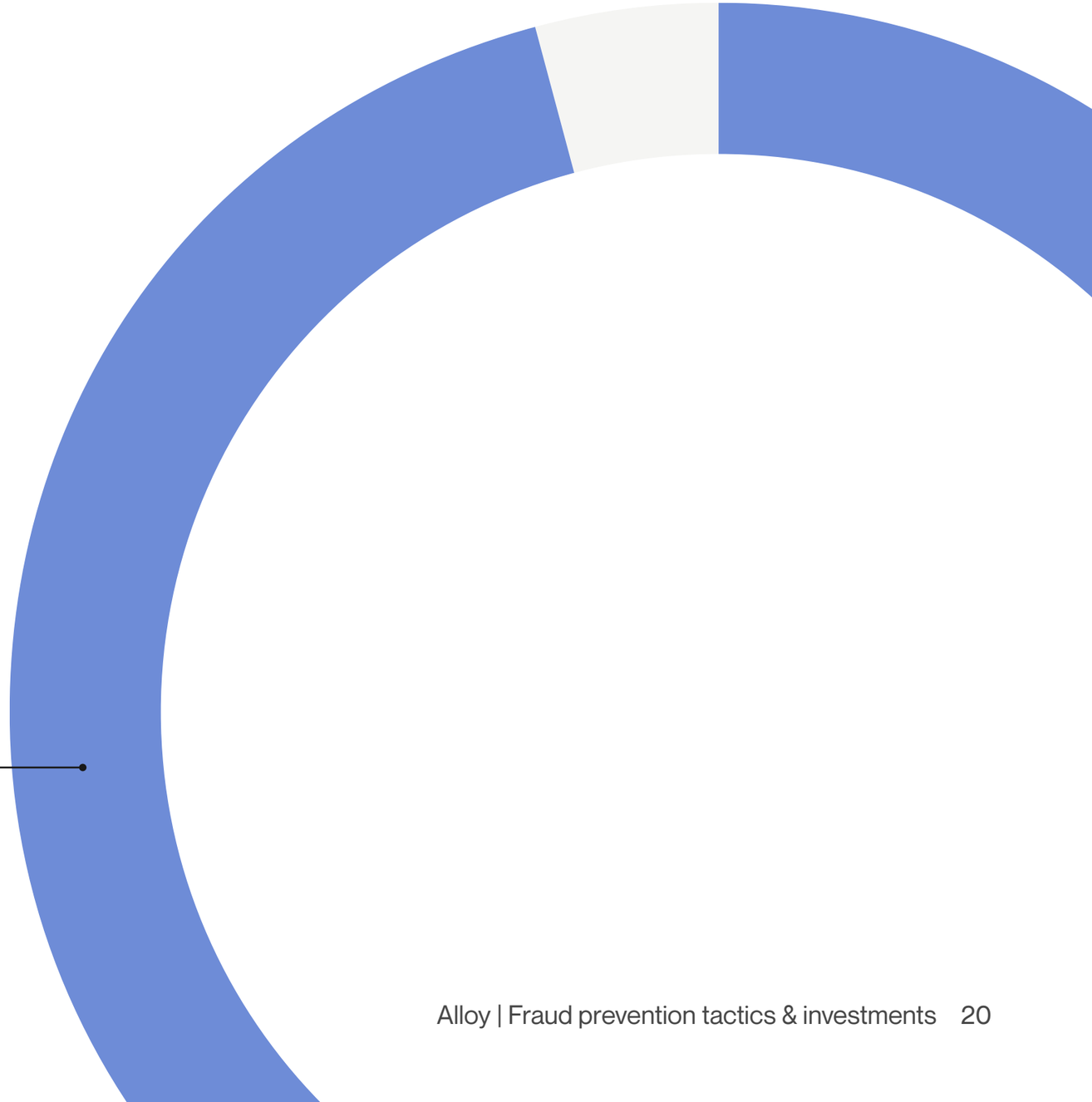
Fraud prevention tactics and investments

Among respondents who felt their organisation was unprepared for growing fraud threats, the top reasons cited were insufficient staff, budget, and tooling/data resources.

Top reasons for fraud unpreparedness

1	Insufficient employees and/or budget for anti-fraud teams	57%
2	Insufficient tooling and/or access to data	57%
3	Current controls are insufficient for combatting evolving fraud tactics	43%
4	Need for greater automation	29%
5	Engineering bandwidth	29%
6	Inability to adapt to new threats	21%
7	Siloed teams in the organisation	21%

With fraud rates rising and regulations tightening, the vast majority of UK fintechs are stepping up their defences.

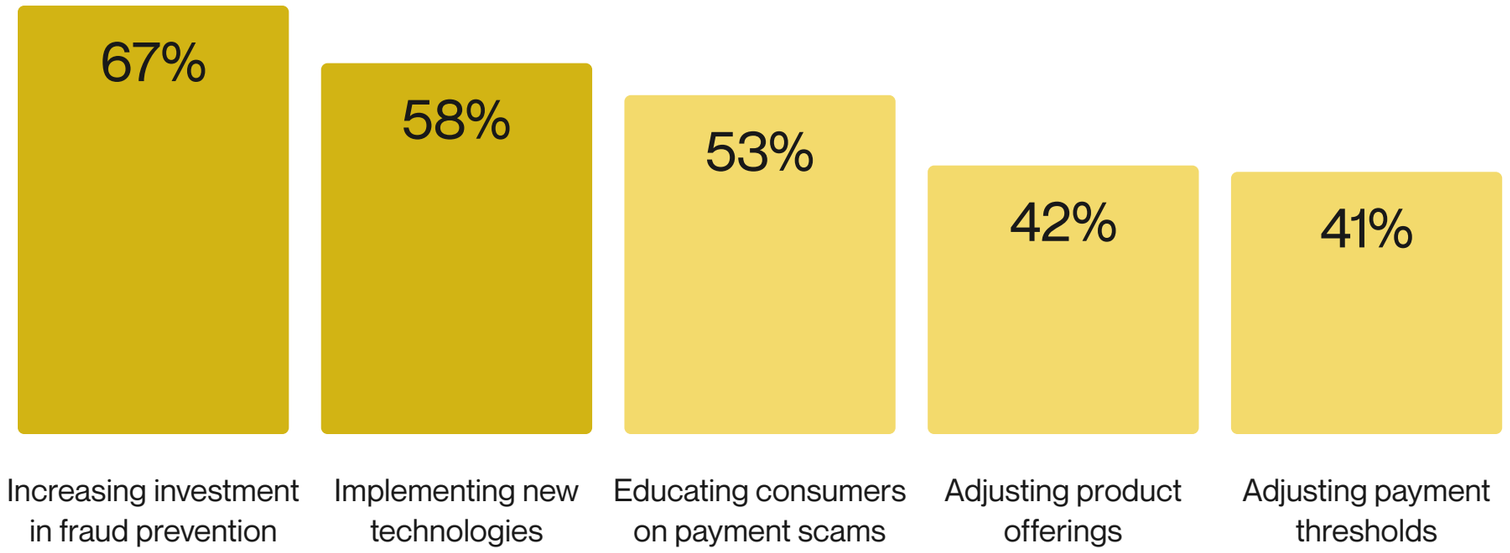


96%

say that their organisation is making **ongoing investments in fraud prevention in 2025.**

The PSR's reimbursement requirements for APP scam victims are driving increased investment in fraud prevention and new tech.

How UK fintechs are responding to the PSR's requirement that payment firms reimburse APP scam victims



Alloy insight

In March 2025, the British government announced that the Payment Systems Regulator (PSR) would be absorbed by the Financial Conduct Authority (FCA). In the near term, the FCA is expected to maintain the PSR's reimbursement requirements for APP scam victims.

96%

of respondents agree that the PSR's requirements for reimbursing APP scam victims stand to have a significant influence over their fintech's overall fraud prevention strategy.

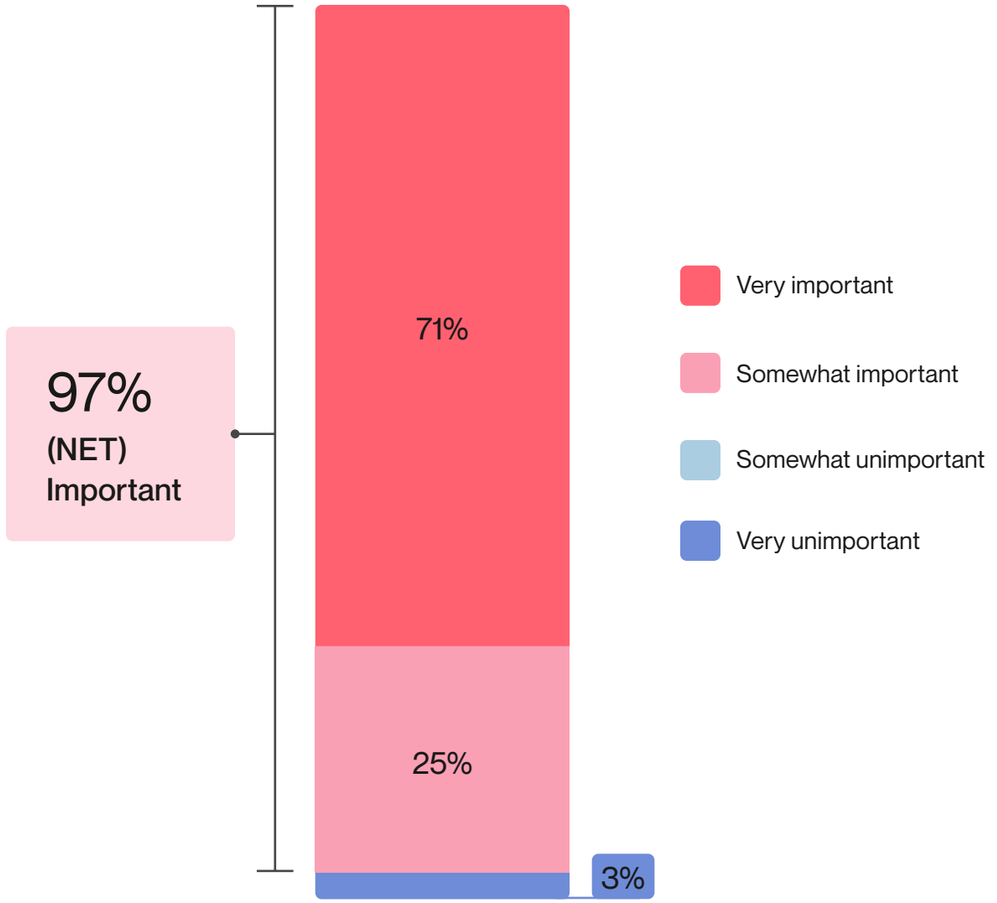
97% of UK fintechs agree that receiving payment service providers (PSPs) must have robust financial crime controls.

Alloy insight

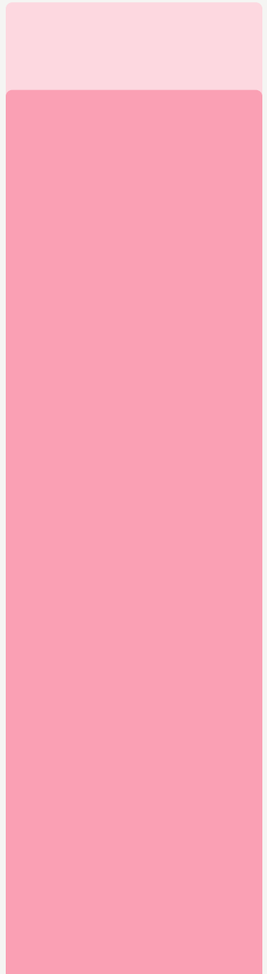
An overwhelming 97% of decision-makers consider the quality of the receiving PSP's financial crime controls to be important when assessing transaction risk.

Under the PSR's regulations, receiving organisations, along with sending organisations, are liable for 50% of the reimbursement if an APP scam is committed, putting the onus on both parties to invest heavily in their prevention infrastructure. A network effect has emerged as a result: As more institutions strengthen their fraud controls, they set new standards for their counterparties. Financial crime controls, then, aren't just a regulatory box to tick, but a requirement to maintaining trusted industry relationships.

When assessing the risk level of a transaction, how important is the quality of the receiving PSP's financial crime controls?



99% of respondents are already using AI to prevent fraud.



91%

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?

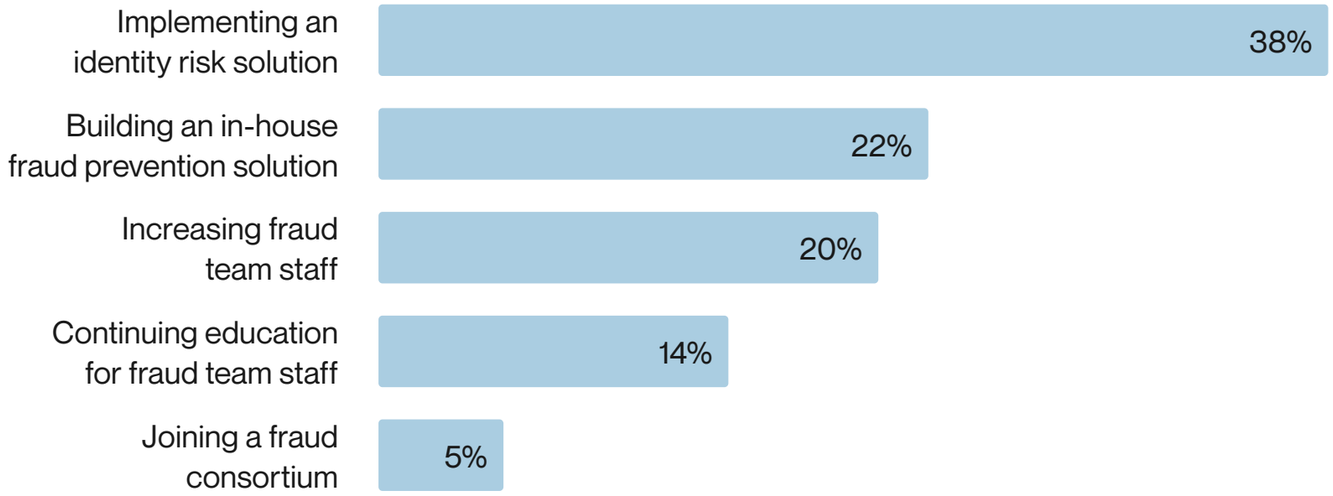
99%
(NET) Use AI

- **75%** — Providing explainability for large data sets, such as providing reasons for why transactions were rejected, or creating narratives for SAR reporting
- **66%** — Supplementing rule-based decisioning with supervised machine learning models (in-house and third-party) to detect anomalous activity
- **64%** — 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

Investments in fraud prevention are paying off, with identity risk solutions leading the way in impact.

Nearly **40%** of UK fintechs 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 organisation over the course of the last twelve months?



92%

agreed that the amount of money their organisation saves thanks to fraud prevention investment outweighs its cost.

In 2025, UK fintechs plan to invest in identity risk solutions and document verification software.

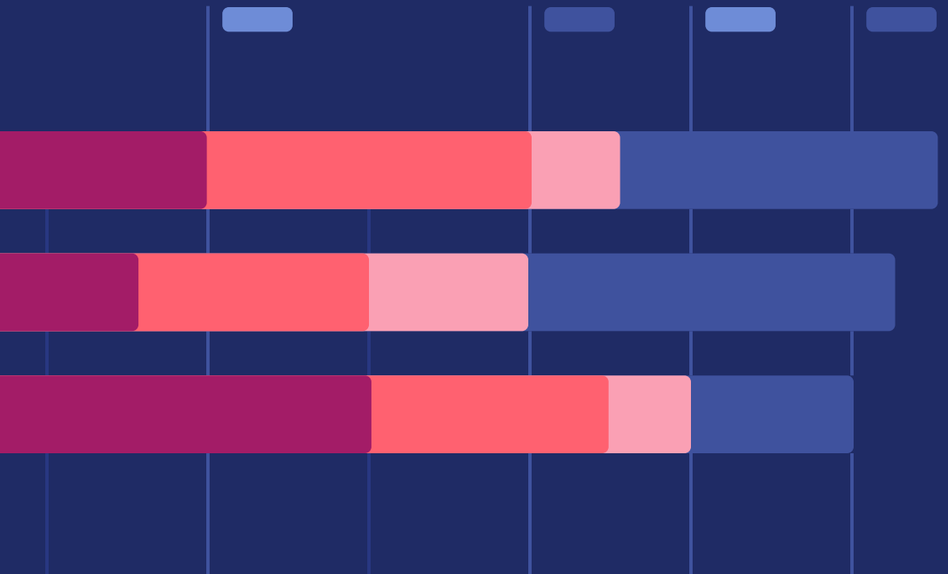
What types of technologies will you be looking to invest in over the next 12 months?

1	Identity risk solution	72%
2	Document verification software	60%
3	Machine learning	47%
4	Anti-scam education tools	47%
5	Voice, facial, and fingerprint recognition	41%
6	Alternative data vendors	33%

Conclusion

Where will financial crime go next in 2025?

A prediction from **James Baston-Pitt**
Head of UK and EMEA at Alloy



In 2025, expect regulators to continue their close scrutiny of the fintech ecosystem. As a result, fintechs must strike a challenging balance between protecting themselves and their customers from fraud while also delivering the frictionless, efficient financial experience that those customers expect.

To achieve both goals, it will be critical for fintechs to adopt a holistic approach to preventing financial crime throughout the customer lifecycle. We'll see more fintechs implement perpetual KYC/KYB policies to turn "in life" risk ratings into a more dynamic and continuous process, rather than enacting periodic look backs that require massive remediation efforts.

To ensure that they can continue to offer the high-quality experiences that their customers demand, fintechs will also need to operate more efficiently by increasing their straight through processing (STP) rates. Especially for fintechs that are expanding into new geographies, increasing STP rates will ensure more genuine customers can access financial products quickly while also enabling fraud teams to zero in on the most credible threats.

Conclusion

With annual financial losses reaching at least £500,000 for four in five UK fintechs, it's clear that organisations have work to do to combat the rising tide of fraud.

At the same time, the UK is home to one of the world's most sophisticated regulatory regimes to combat fraud. Measures by the newly merged Payment Systems Regulator and the Financial Conduct Authority to protect fintechs and their customers from bad actors are being watched by regulatory counterparts around the world. The PSR's mandatory reimbursement rules for APP fraud cases are eliciting a unique change — not only in how fintechs equip themselves and their customers against fraud but also in what they expect from the receiving banks or payment service providers. Shouldering 100% of the financial loss equally between sending and receiving institutions encourages fintechs to strive for best practices in fraud prevention and to demand the same from their competitors and partners.

However, domestic regulatory innovation cannot solve the problem alone. The financial crime rings that dominate the fraud world are geographically diverse and agnostic about where they target. This creates challenges for all fintech companies, particularly those that want to operate internationally or extend their services to non-UK customers. Negotiating multiple regulatory regimes against a backdrop of AI-driven fraud is a constant pressure. It's no wonder, then, that regulatory fines and penalties preoccupy the majority of C-suite fintech decision-makers.

Still, organisations have reason to be optimistic. Nine in 10 UK fintechs agree that what they save from fraud prevention investment outweighs its cost. Many fintechs still need to equip themselves with more talent, tools, and technology to improve fraud preparedness, but it's encouraging to see many already taking steps to better prevent fraud and financial crime for their customers.

Report snapshot

UK fintech 2025 snapshot

67%

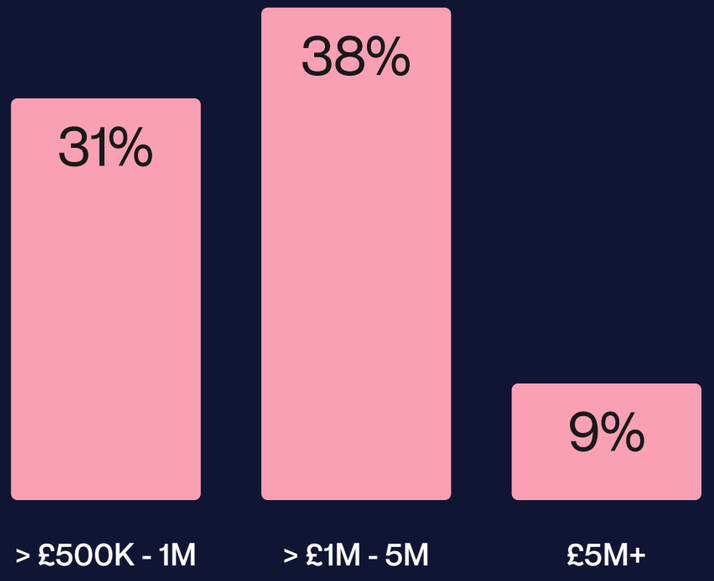
of repondents saw an increase in fraud events YoY

Top investment for 2025

72%

Identity risk solution

Direct fraud losses



Top fraud consequences

Reputational damage	85%
Financial loss	84%
Legal issues	84%
Fines/penalties	84%

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.

Alloy UK launched in January 2023, with offices in London. Today, the team partners with 20+ EMEA headquartered clients.

Learn more at alloy.com/uk