

*FS*tech

In collaboration with



Bottomline®

Fraud intelligence in financial services: Investment drivers, AI adoption and consortium strategies



Introduction

Financial services institutions (FSIs) face a constant battle against fraudulent activity, which threatens their customers and reputation. Whether driven by organised campaigns or the scattered actions of opportunistic criminals, fraud creates a persistent source of losses, concern, and organisational pressure for customers and FSIs alike.

One way to share this burden is by joining fraud data-sharing consortia, industry bodies through which financial institutions and relevant third-party organisations can share anonymised fraud data to collaboratively improve sector-wide detection efforts and strengthen their own response to fraudulent activity. These arrangements bring their own benefits and drawbacks like any other security programme, and participation comes down largely to organisational appetite.

To better understand how FSIs are tackling rising fraud risk, FStech and Bottomline surveyed financial leaders about the primary challenges they face. The research examines the key factors driving investment in fraud

intelligence, including persistent fraud campaigns, regulatory pressure, and the potential benefits of modernising fraud detection and prevention.

The research also explores how fraud data-sharing consortia can complement internal fraud intelligence strategies. The findings reveal a tension among respondents, with many recognising the potential for consortia to improve fraud detection through broader access to fraud data, while also expressing concerns about the legal, regulatory, and operational implications of participation. A primary focus of the research is the role of AI in fighting fraud, including the use cases financial leaders consider most valuable, how comfortable they are with AI being embedded in fraud workflows, and limitations they associate with greater adoption. Overall, the results illustrate a fraud intelligence landscape undergoing significant change. Organisations see potential benefits in both consortia participation and AI adoption, but concerns around cost, data privacy, regulation, explainability, and integration are shaping how quickly and how extensively they are prepared to adopt new approaches.



Methodology

FStech and Bottomline surveyed 204 financial services decision-makers specialising in fraud intelligence operations and risk.

Throughout the research, respondents were prompted to register their primary interests and concerns surrounding strategic investments in fraud data-sharing consortia and AI, as well as the wider fraud trends shaping their strategies.

Respondents represented a diverse mix of organisations across the financial services sector, including major retail banks, insurance providers, and building societies. Responses were collected from

organisations in the United Kingdom, United States, Belgium, Finland, Netherlands, Norway, Portugal, Sweden, and Switzerland.

In total, responses were collected from 101 respondents based in the US and 103 in the rest of the world. Unless otherwise stated, the figures presented at the beginning of each section represent the combined results from UK and rest of world respondents. The analysis also examines differences between the two markets where relevant.

Please note: Percentages may not total 100 per cent due to rounding or multiple-choice questions.

Key findings:



Daily fraud drives investment:

Regular attacks such as authorised push payment and card not present fraud are the most common drivers of investment, as cited by over a third of respondents. While trying to reduce these consistent threats remains a primary motivator, other pressures such as internal risk audits and the increased focus on real-time risk by regulators makes fraud tech modernisation a particularly strong focus for many FSIs.

“Persistent, day-to-day fraud threats remain the primary driver of investment, while regulatory demands and real-time payment initiatives are increasing the urgency for modernisation.”



Consortium participation is dependent on risk appetite:

Although 41 per cent of respondents see improved fraud detection accuracy as a clear benefit of participating in a fraud data-sharing consortium, many still question risks involved. Over a third of respondents, 39 per cent, see legal and regulatory uncertainty as a blocker for participation, while cost and other operational barriers also remain significant concerns for many.



FSIs value tangible results over long-term technical improvements:

The most commonly cited benefit for anti-fraud AI deployment among respondents was real-time anomaly detection at 44 per cent. This reflects a clear desire by FSIs to put AI to work in areas where its speed and analytical capabilities can deliver tangible improvements, before considering more autonomous applications.



Full automation is still not the goal:

Just 9 per cent of respondents said AI should operate autonomously without human involvement within fraud detection and prevention. Meanwhile, 60 per cent selected AI operating models focused on supporting analysts, making recommendations, improving operational efficiency or reducing false positives, indicating a continued reluctance to deploy AI without strict human oversight.



AI is the investment focus:

The most common response for how FSIs expect their fraud intelligence strategy to evolve over the next two years is a shift towards AI-led automation, with 45 per cent selecting this option. With just 20 per cent stating they do not expect to make significant changes to their fraud strategy, the findings indicate that a clear majority of respondents expect their approach to fraud intelligence to evolve over the next two years.





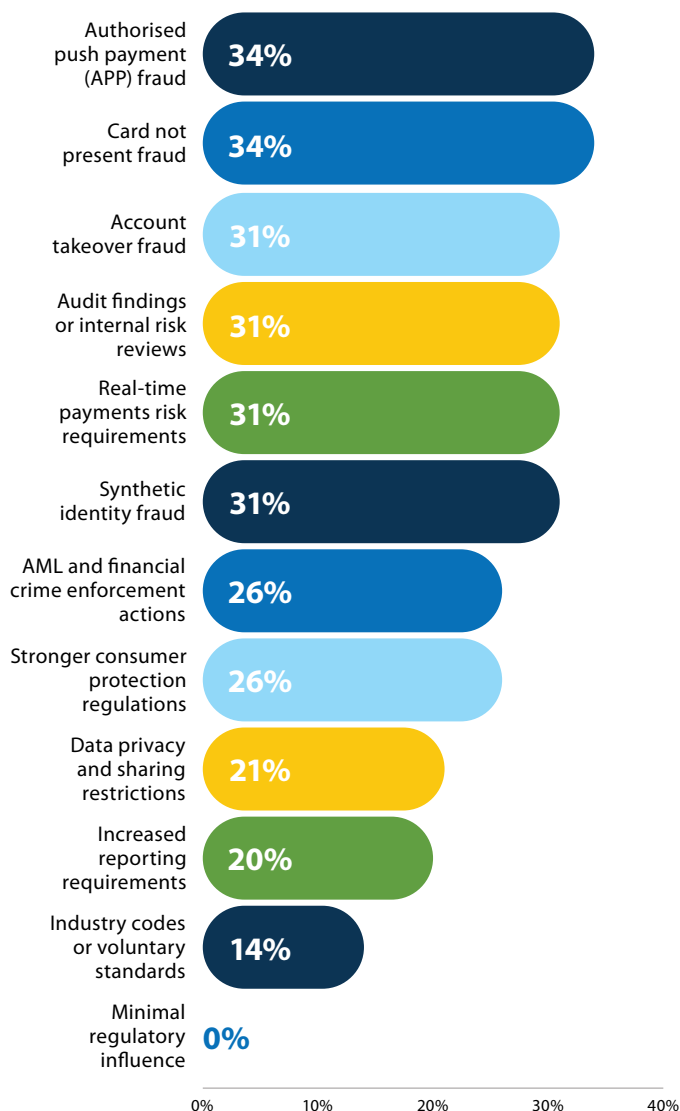
Contents

1. Established threats drive investment pressure	5
2. Growing interest in data-sharing consortia	6
3. Chasing performance through consortium participation	7
4. Risks and hurdles: When consortia aren't a possibility	8
5. From low maturity to gradual fraud convergence	9
6. Where AI can deliver value for fraud teams	10
7. The strategic focus for AI adoption	11
8. Black box worries: The problem of AI data risks and explainability	12
9. How to sell safety: The optimal models for fraud intelligence	13
10. From manual remediation to real-time automation	14
11. Conclusion	15

1. Established threats drive investment pressure

Like the wider cybersecurity environment, the fraud landscape is becoming increasingly complex, with financial institutions facing persistent threats alongside growing regulatory and operational pressures. For FSIs, established forms of fraud remain a core concern. Over a third (34 per cent) of respondents said authorised push payment fraud and card not present fraud most influence their fraud investment decisions, both decade-old attack types that continue to impact the financial services sector. Account takeover and synthetic identity fraud were also significant factors, both cited by 31 per cent of respondents.

Which fraud trends, regulatory, or external pressures most influence your fraud investment decisions? (Select up to three options)



Importantly, these attacks can be the work of either organised threat groups or individual fraudsters acting on their own. This makes them more of a fragmented target to tackle, as attacks of this kind might not be forewarned through wider sectoral threat data.

The research indicated that proactive pressure is also a significant factor influencing their fraud investment decisions. Respondents said that both audit findings or internal threat reviews and real-time payments risk requirements were major drivers for investment, logging 31 per cent for each option.

This implies that many leaders are looking to organisation-specific risk indicators, as well as external requirements around real-time payments, to form the basis for their investment decisions. The conclusion appears to be that their fraud tech is either not fit to deal with the volume of real-time threats or not capable of meeting evolving requirements, informed by sector-wide fraud data, showing real-time threats are a necessary area of investment. Where FSIs are met with non-mandatory external pressures, such as industry codes or voluntary standards, a far smaller proportion say it affects their investment decisions, with just 14 per cent saying they do in the survey.

All of this paints a picture of FSIs investing to achieve improvements to their anti-fraud operations where possible to cover the day-to-day pressures of repeat fraud incidents and, to a lesser extent, to meet regulatory requirements. Even within this subset, organisations are more likely to be influenced by external requirements where they are linked to specific operational or consumer protection needs.

Overall, the findings suggest that persistent fraud threats remain the strongest driver of investment, while internal risk assessments and requirements around real-time payments are also significant factors. Broader industry initiatives appear to have less influence on investment decisions.



2. Growing interest in data-sharing consortia

Fraud data-sharing consortia are well-established in the financial services industry, but the degree to which organisations are already participating in them varies widely. The more organisations signed up to consortia, the more accurate, timely, and rich their information. But joining is not always a simple process and, for some organisations, comes with clear drawbacks that deter participation altogether.

A sizeable portion of respondents acknowledged the positive values in fraud data-sharing consortia and have recognised this by taking part in, or leaning towards, participation. Over a third of (35 per cent) of respondents are either already participating in consortia or evaluating joining one, with 10 per cent of respondents already actively participating in multiple. Although there is clear positive sentiment towards consortia in the sector, it is also clear that some organisations have already discounted participation altogether because they have deemed it too high a risk.

Some 11 per cent of respondents said they cannot participate in consortia at all due to regulatory restrictions. These groups may be the hardest to reach, as while their responses do not preclude interest, they do indicate entrenched regulatory red lines and dependencies that could prove extremely difficult to overcome. **US respondents were more likely to fall into this group, with 15 per cent indicating regulations block consortia participation compared**

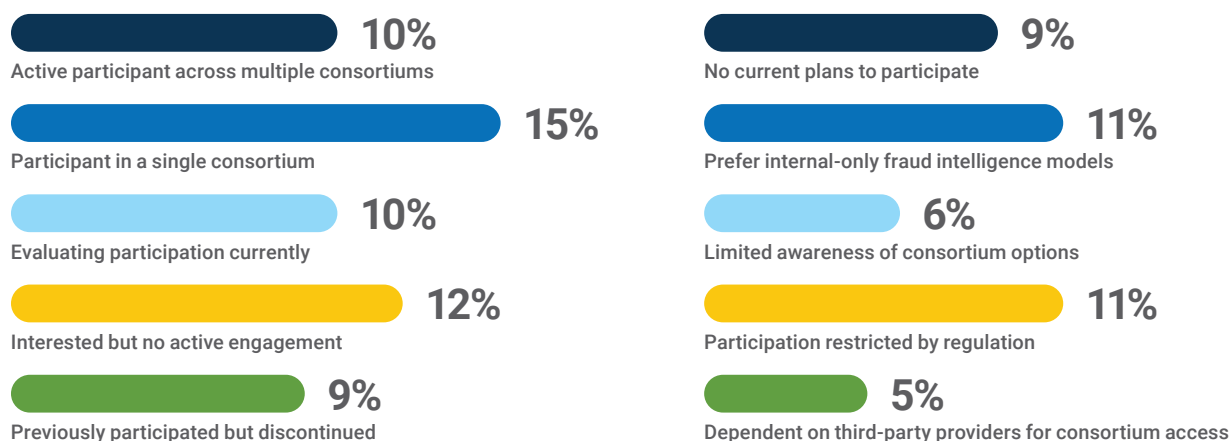
to 8 per cent among those in the rest of the world.

This is reflective of diverging regulatory landscapes in different regions, with regional laws acting as barriers to territory-neutral sector data-sharing agreements.

A further 9 per cent said they have previously participated in fraud data-sharing consortia but have since discontinued their membership. This is another hard cohort to reach and win around, as they come with set opinions on the downsides to fraud data-sharing consortia that for them were enough to justify ceasing their participation.

Together with the regulatory holdouts, the data suggests a fifth of all FSIs are likely to resist participation at least until ground truths about consortia membership change or their organisational circumstances do. Nevertheless, respondent sentiment indicates there is strong potential for participation numbers to increase significantly. Among those respondents not already a member of a fraud data-sharing consortium, 12 per cent said they are generally interested in but not currently pursuing participation and a further six per cent said they have limited awareness of fraud consortium options. This is fertile ground for current consortia, provided benefits are clearly expressed and communicated in a manner that cuts through to leaders who are holding out or unaware of their options.

How would you describe your organisation's participation in fraud data-sharing consortia – shared bodies in which financial institutions and relevant third-party organisations share anonymised fraud data and wider risk intelligence, to improve collective detection and response efforts? (Select one option)

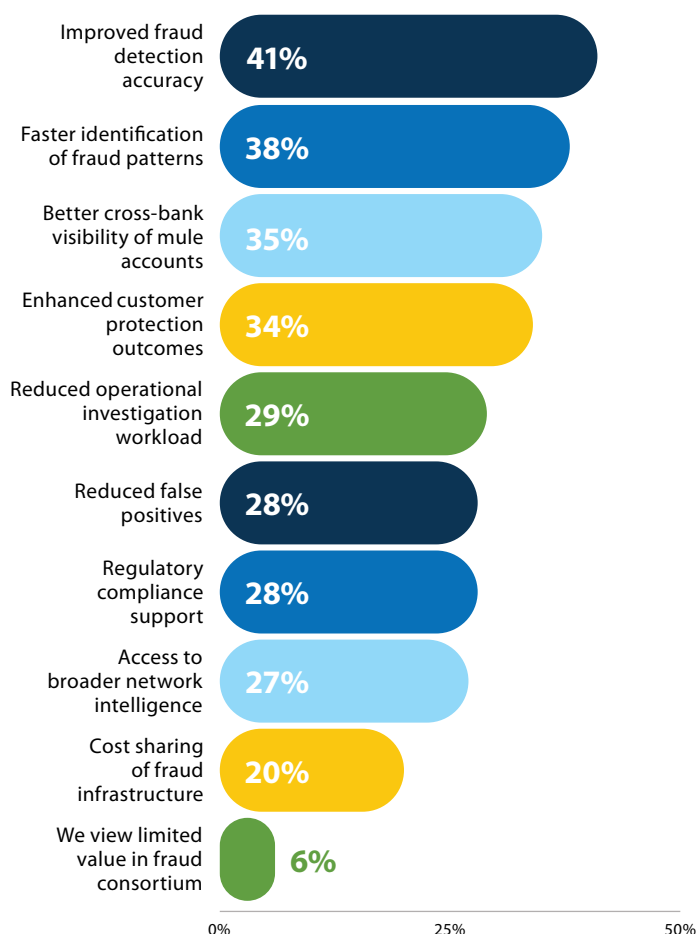


3. Chasing performance through consortium participation

Why this matters: Interest in consortium participation is already significant, but broader adoption depends on trust, transparency, and perceived risk. Financial institutions need greater confidence that data-sharing models protect confidentiality, satisfy regulatory requirements, and deliver measurable fraud-prevention outcomes.

One of the chief benefits of joining a fraud consortium for financial organisations is collaborative intelligence sharing. Organisations in these groups share structured data in near real time, helping participants to build an up-to-date, accurate picture of the latest fraud activity. The chief strength here is not just the breadth of data, but the improved resolution that comes with aggregated threat data as well as the speed at which APIs allow standardised data to be shared within a consortium.

What do you view as the main value drivers for participating in a fraud consortium? (Select up to three options)



Respondents indicated that this is a clear draw for participating in a consortium, with 41 per cent saying improved fraud detection accuracy was a main value driver and 38 per cent pointing to faster identification of fraud patterns. These are measurable improvements that make an immediate impact on the day-to-day operations of any FSI and the safety of their customers.

Regional comparison reveals that US respondents favour accuracy more than their global peers, with 46 per cent choosing it as a primary value driver compared to 36 per cent among responses from the rest of the world. Respondents from the latter cohort favoured faster identification, with 42 per cent choosing it as a value driver.

Whether speed or accuracy are the focus, these benefits are extremely difficult to achieve outside of a consortium, as they rely on analysis of data at a scale and speed that is not generally possible when solely reliant on internal threat data.

A further 35 per cent highlighted the benefits a consortium could offer for identifying and tackling mule accounts, criminal holdings used to hold and transfer illegally obtained funds. While the top two options relate to tackling fraud in real-time, the impact fraud data-sharing consortia can have on mule accounts is a longer-term effect that makes the overall sector safer by ridding it of criminal infrastructure.

In contrast, respondents saw less value in cost sharing of fraud infrastructure and access to broader network intelligence, with just 20 and 27 per cent choosing them respectively. This implies that FSIs place more value on consortium offerings that tie directly into fighting fraud rather than those that offer wider organisational benefits such as reducing the cost of anti-fraud operations or providing broader network intelligence. FSIs may see data sharing as an unnecessary activity altogether if it is not pegged to demonstrable business benefits, whether this means reduced fraud activity and improved customer safety, or actionable insights for improving their fraud setup as informed by anonymised sectoral data.

In all, the findings show FSIs are more drawn by the quantifiable benefits of fraud data-sharing consortia over the longer-term benefits such as reduced cost. By a margin, respondents chose aspects of consortia that directly benefit their day-to-day anti-fraud teams.

4. Risks and hurdles: When consortia aren't a possibility

For all the benefits of fraud data-sharing consortia, financial organisations must consider a range of organisation-specific pros and cons when they decide whether or not to participate in them.

The responses indicate that while organisations recognise the potential benefits of fraud data-sharing consortia, many are still held back by their risk appetite or simply the regulatory reality of their sector. Among respondents, the most likely factor to block consortium participation was legal and regulatory uncertainty, at 39 per cent. This is markedly higher than the number of respondents who indicated they are explicitly banned from participating due to regulation, reflective of a need for better communication around how consortia fit in with legal requirements and simplification of the rules surrounding fraud data-sharing consortia. A closely related concern that respondents said holds them back from participating was that of how it could implicate their data privacy and confidentiality stature, with 36 per cent of respondents saying so.

Almost one third of respondents (32 per cent) said the costs associated with taking part in a fraud consortium were a concern that could block participation. Given that the cost-sharing benefits of fraud data-sharing consortia were a draw for a markedly low number of respondents, this implies that the up-front costs of joining a consortium continue to be a blocker.

The costs of joining must always be balanced with the potential commercial benefits of participation, and

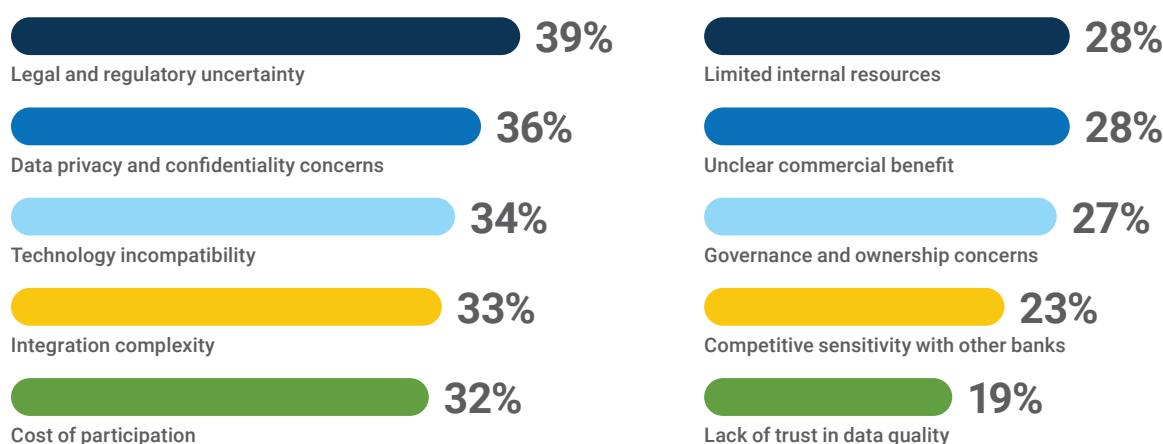
here another regional variation stands out. **Nearly one third of US respondents, 32 per cent, said the unclear commercial benefits of participation are a blocker, compared to 25 per cent among respondents from the rest of the world.** This could indicate a need for more visible demonstrations of the value of fraud data-sharing consortia in the US, to provide real-world examples for the value of participation.

Among respondents who indicated that they had been in consortia but left, the most commonly cited blocker was technological complexity, with 12 of the 18 respondents in this category stating it prevented their participation. This represents two-thirds of those who had previously participated but discontinued their membership. More broadly, technological incompatibility was chosen by 34 per cent of all respondents, while 33 per cent cited integration complexity.

These answers are closely associated with those on cost and internal resources: all paint a picture of an FSI recognising it cannot meet the technical requirements necessary for participation without expending undue time, effort, or budget.

All of this shows that consortium participation continues to be hampered by unknowns. To expand uptake, more transparent conversations need to take place over the regulatory implications of joining a consortium, how they uphold the data privacy standards, and what is being done to ensure the costs match the potential benefits.

Which factors are most likely to block consortium participation? (Select up to three options)



5. From low maturity to gradual fraud convergence

Financial services organisations continue to operate fragmented fraud, anti-money laundering (AML) and sanctions capabilities, with many adapting to the changing threat landscape through a patchwork of legacy systems, outsourced analytical functions, and unified fraud platforms.

Few respondents indicated they already have already converged their fraud, AML, and sanctions capabilities. As many respondents said they have a fully integrated financial crime platform – 12 per cent – as said they have no formal integration strategy whatsoever, with the majority of respondents indicating only one to two of the three are fully integrated.

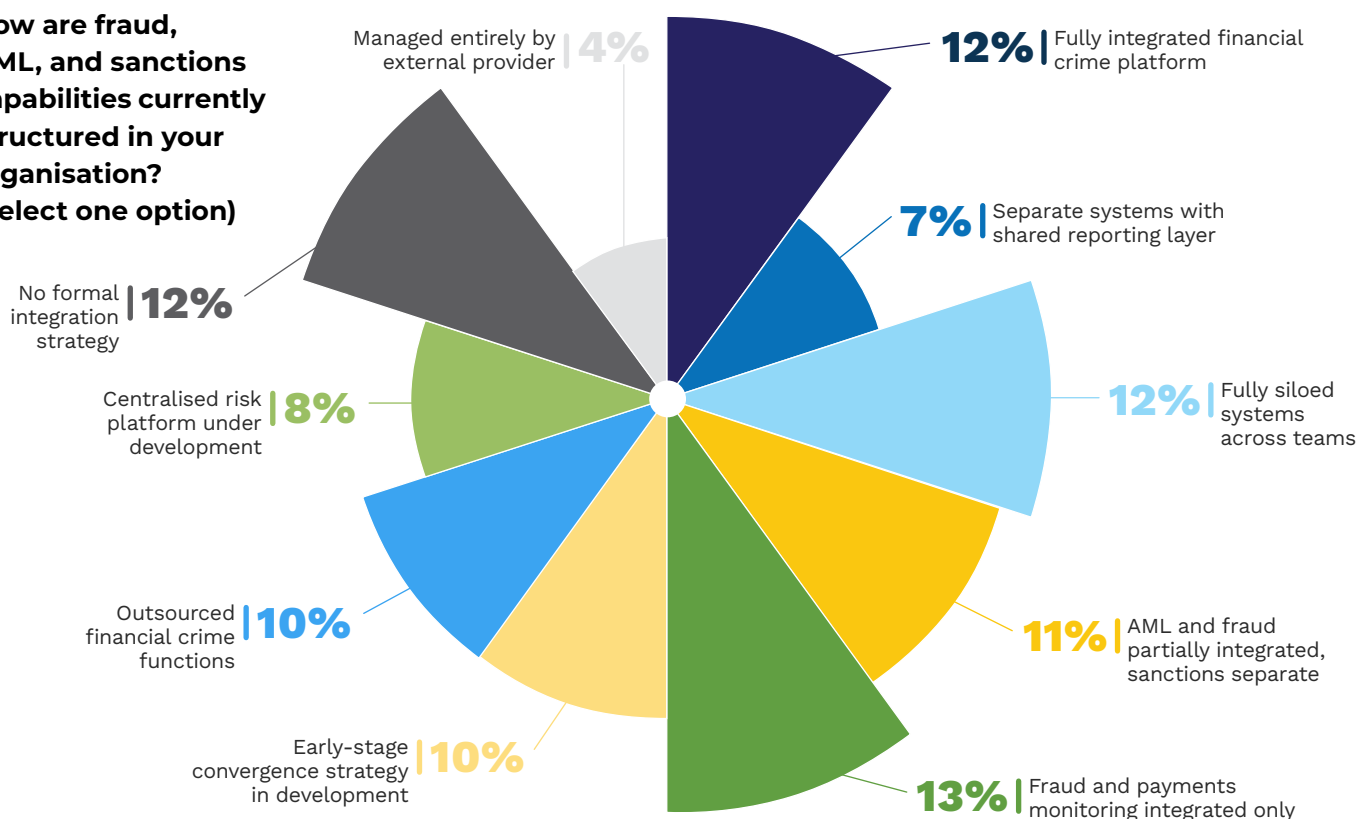
This shows the significant challenge that many firms face when attempting to build a holistic picture of the fraud incidents their customers face. Without a fully integrated financial crime platform that allows different teams and business segments to share and draw on centralised threat data, organisations will miss key fraud indicators. Organisations with a low level of fraud centralisation and integration may also find it more difficult to harness the full benefits of technology such as AI, which requires as much data as possible to produce accurate, detailed analysis of fraud incidents as well as to identify anomalous behaviour from the baseline.

This also highlights the immediate benefits fraud data-sharing consortia can offer many businesses, as bulk data from across the industry is shared that can fill any gaps left by a fragmented internal approach to structured data collection and analysis.

Despite the generally fragmented picture, the survey data shows a clear trajectory of improvement for centralised, fully integrated fraud, AML, and sanctions capabilities. Some 10 per cent of respondents said they are in the early stages of converging disparate fraud capabilities, while a further 8 per cent said they are actively developing a centralised risk platform. Taken together with those who already possess a centralised system, almost one third of respondents (30 per cent) are either in a strong position with their fraud systems or headed in that direction.

As a unified approach becomes more commonplace, FSI will be in a better position to target other fraud strategy shifts outlined in the research such as consortium participation and AI adoption. In this sense, the trend towards convergence is a positive indicator for the medium-to-long-term likelihood of a majority of FSIs investing more in modernising their fraud capabilities.

How are fraud, AML, and sanctions capabilities currently structured in your organisation? (Select one option)

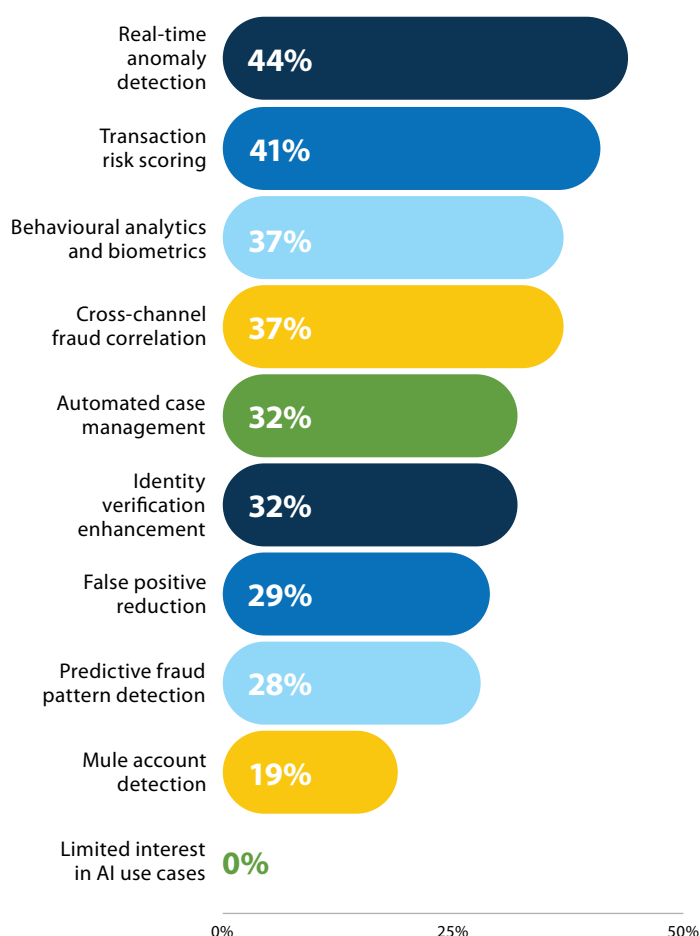


6. Where AI can deliver value for fraud teams

Why this matters: Financial institutions are focusing on AI applications that deliver immediate operational benefits, including real-time anomaly detection, transaction risk scoring, and cross-channel correlation. This highlights the importance of positioning AI as a practical tool for improving fraud detection rather than a purely long-term innovation initiative.

Financial leaders are clear that AI can play an important role in improving fraud detection, with zero respondents indicating limited interest in AI use cases. Whereas traditional AI systems such as machine learning algorithms have historically been used as a post-incident forensics tool, newer applications of AI can play a more active role in identifying and preventing fraudulent activity in real-time.

Which AI use cases are most important for fraud detection improvement? (Select up to three options)



Indeed, AI systems can use the high-speed information sharing from multiple sources to build connections between disparate points of data and produce a sector-wide picture of emerging fraud threats faster than a human could. Respondents specifically highlighted real-time anomaly detection as a core use case for AI, with 44 per cent selecting it as one of the top three use cases for the technology.

A nine-point variance emerged among respondents in their appetite for real-time anomaly detection, with 40 per cent of US respondents citing it as a top three use case compared to 49 per cent from the rest of world.

This is consistent with the greater focus of speed over accuracy among non-US respondents indicated in question three.

Transaction risk scoring was the second-most selected at 41 per cent, while behavioural analytics, biometrics, and cross-channel fraud correlation trailed close behind at 37 per cent. The throughline with these use cases is clear: all are tasks that befit the data throughput and analytical powers of AI models, which can draw out semantic links from reams of fraud data that a human worker would struggle to identify. The speed and accuracy improvements achievable through AI are becoming increasingly important as attackers make use of the technology, raising the bar for fraud detection and remediation. Automated fraud campaigns already operate at speeds and breadths that human workers will struggle to fight, which raises the value of using AI to identify and respond to fraudulent activity. The focus on capabilities suited to AI is further validated as FSIs face down this threat. On the other side of the scale, respondents placed less importance on using AI for tasks such as mule account detection, with just 19 per cent of respondents choosing this as one of their top three use cases. This does not mean mule accounts are seen as an unimportant issue, as the responses to question one made clear, but rather highlights the additional importance they place on core anti-fraud functionality for which AI systems can be used. At a fundamental level this underlines the urgency with which FSIs are approaching this issue. Rather than the drawn-out digital transformation one might expect to see in such a regulated industry, financial services leaders are seeking AI systems that can get them up to speed with the most advanced threats they face.

7. The strategic focus for AI adoption

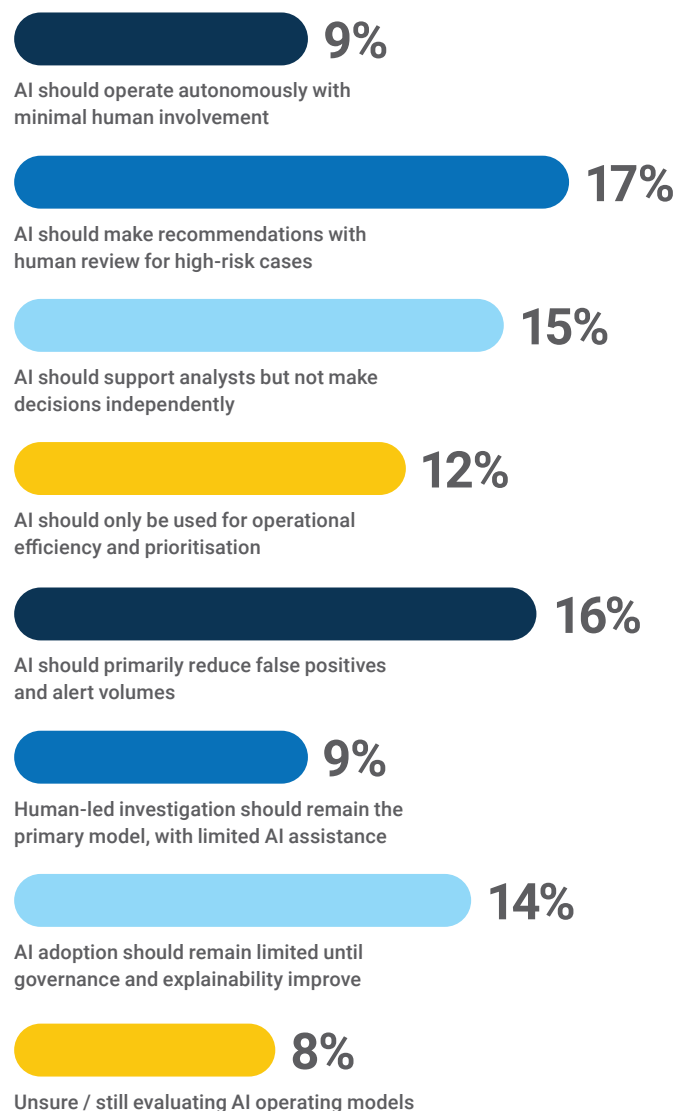
Two important factors are at play in the responses to this question. First, in financial services speed of adoption never comes at the expense of safety or regulatory obligations. Second, AI systems are not homogenous and nor can they be deployed in a one-size-fits all manner. Regardless of their intended use cases for the technology, each organisation will seek to integrate AI into their software stack to a different degree and with a different outcome in mind, and this is no different when the technology is applied to fraud.

The result is a wide variety in the manner in which respondents seek to deploy AI for fraud detection. Taken together, 60 per cent of respondents selected an operating model in which AI supports analysts, makes recommendations, improves operational efficiency or reduces false positives, rather than operating fully autonomously. This indicates a preference for using AI to improve productivity and decision-making while retaining human oversight. Areas leaders are confident that AI can play a role include reducing false positives, selected by 16 per cent of respondents, as well as generating recommendations for high-risk cases that can then be actioned by human analysts. This is in line with the key benefits of the technology as outlined earlier in the survey, namely the speed and scale at which AI systems can identify potential anomalies and compare them against broader data sets to flag them as either real threats or false positives. Just nine per cent of respondents want AI to operate fully autonomously across their fraud detection and prevention workflows, indicative of the inherent distrust in the technology at its current level of maturity. Indeed a greater proportion, 14 per cent, stated that they are targeting limited AI adoption until the technology is more explainable. This is an issue of compliance more than technical ability, implying leaders need the technology to stand up to regulatory scrutiny and pass the test of stakeholder questioning.

These responses make clear that the potential benefits of AI, and urgency with which FSIs are feeling to deploy it, are not enough to entirely quell fears of its use. As the next section makes clear, these fears are alive in the minds of financial services leaders, demanding robust reassurances from those who seek to provide them with the AI and platforms they require.

Institutions that invest less in commercial fraud controls may inadvertently create wider systemic risks, particularly as fraud becomes more interconnected and capable of spreading across supply chains and shared infrastructures. A more balanced model that combines strong institutional safeguards with informed and engaged clients is likely to deliver better outcomes for both sides.

How should AI ideally operate within fraud detection and prevention workflows? (Select one option)

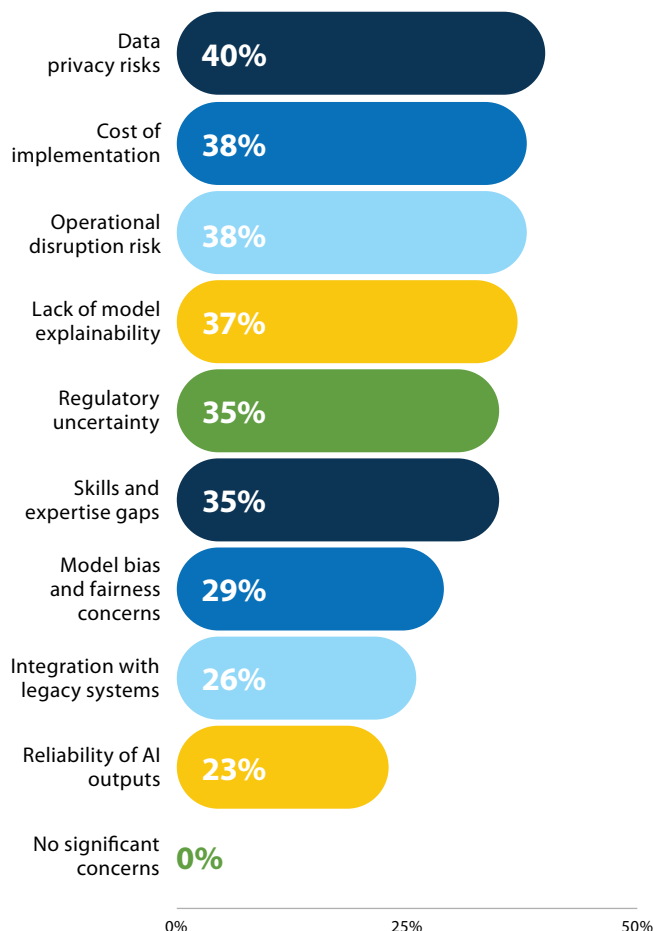


8. Black box worries: The problem of AI data risks and explainability

Why this matters: Successful AI adoption will depend as much on trust as on technical capability. Concerns around privacy, cost, operational disruption, explainability, and regulatory uncertainty must be addressed before institutions move from pilot programs to broader deployment.

As the previous answers make clear, respondents recognise AI as an accelerator for fraud detection and prevention. The technology has clear benefits, bringing greater automation, speed to detection, and powerful analytical capabilities to bear. However, AI also presents inherent challenges and risks that must be averted before they come to fruition, or FSIs face disruptive, costly, and potentially legally perilous consequences.

What are your main concerns regarding AI adoption in fraud detection? (Select up to three options)



Data privacy risks are a commonly cited concern when using AI for enterprise use cases, as without total oversight of how data is processed and stored when passed to an AI model, organisations can't be entirely confident that their data will remain private.

Indeed, data privacy risks ranked highly among responses for this question, with 40 per cent of respondents citing this as one of the top three concerns associated with the technology. The stake here for FSIs could hardly be higher, as information associated with fraud incidents typically contains highly sensitive data linked to the FSI, its clients, or both.

Respondents were as worried about the cost of implementing AI systems as they were the potential operational disruption these systems could cause, with 38 per cent citing each as key concerns. This highlights the tension inherent to discussions around AI, with leaders eyeing the outlay necessary to deploy coherent systems that integrate with their existing setup and wondering how long until they achieve meaningful return on investment.

Some concerns were limited to specific regions: skills and expertise gaps, for example, were cited as a concern by 38 per cent of non-US respondents, while 33 per cent of US respondents said the same.

This implies that the concerns organisations have with advanced technologies like AI can closely follow their access to domestic workers with the skills necessary to make the most of them.

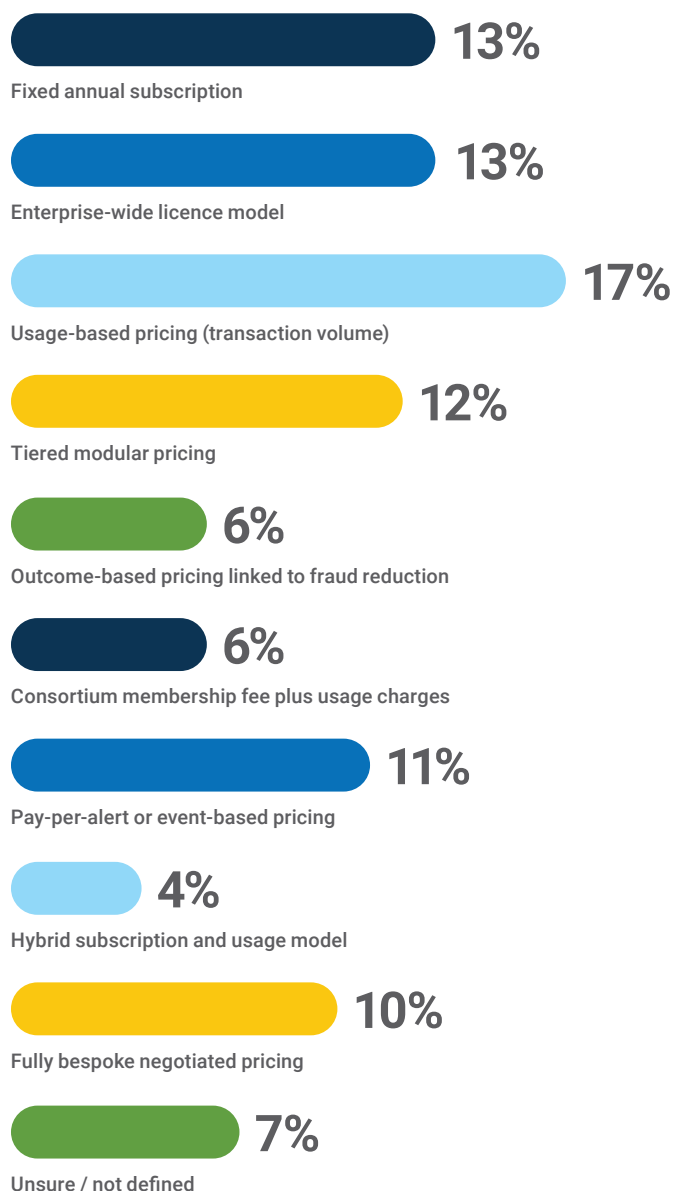
A similar proportion, 37 per cent, cited lack of model explainability as a key concern. This is more than double the 14 per cent who, in question 7, said explainability was a blocker for AI deployment, suggesting that while this concern is widespread it does not always translate into a decision to limit implementation. This is primarily a concern of data quality and lack of strategic accountability. AI models that cannot provide an auditable explanation for why they produced certain data or made specific decisions come with an inherent lack of trust and may prove inadequate for an area as heavily regulated as automated fraud detection. This is not a concern that disappears at point of adoption, either. Without a clear decision tree for outputs, leaders could reasonably question whether they can trust the models' decisions, particularly in high-risk cases.

9. How to sell safety: The optimal models for fraud intelligence

The survey data suggests that organisational expectations for how fraud intelligence platforms are priced are varied, reflecting the different ways FSIs expect to use these technologies.

The single most popular answer among respondents was usage-based pricing linked to transaction volume, at 17 per cent. This reflects the desire among FSIs to align the cost of fraud intelligence platforms with the scale of their operations, allowing organisations to pay according to the volume of activity being monitored.

What pricing model is most aligned with your organisation's expectations for fraud intelligence platforms? (Select one option)



Some respondents went further in suggesting their organisation should only pay when a specific condition is met: 11 per cent said they seek pay per alert or event-based pricing, while six per cent seek an outcome-based model pegged to rates of fraud reduction. Though a minority, this indicates that a subset of respondents are still hesitant to spend on any solution unless there is a clear link between the cost and their efforts to tackle fraud.

Over one quarter (26 per cent) expect fraud intelligence platforms to be available at one price point, either in the form of a fixed annual subscription (13 per cent) or enterprise-wide licence model (13 per cent). A further 12 per cent favour tiered modular pricing, suggesting that a significant proportion of FSIs want pricing structures that give them flexibility over the scale or scope of the technology they deploy.

The data shows FSIs expect to see clear value from their fraud tech investments, with the largest group of respondents favouring pricing linked to their level of usage and others preferring models that provide greater predictability or flexibility over costs.



10. From manual remediation to real-time automation

The extent to which respondents see their fraud intelligence strategy changing over the next 24 months is reflective of the appetite for new technology such as AI measured throughout the survey, as well as the improvements that technology and data consolidation can unlock. A significant chunk of respondents indicated they expect to shift toward AI-led automation over the next 24 months, with 45 per cent selecting this as a core change they expect to see. With the fraud landscape evolving quickly and new threats such as AI-powered fraud becoming more common and sophisticated, this degree of short-term change and willingness to modernise is consistent with the appetite for AI measured elsewhere in the research.

Over half of non-US respondents, 51 per cent, indicated they would pursue AI-led automation over the stated period, compared to 39 per cent of US respondents.

This 12-point gap could be indicative of greatly increased appetite among FSIs in the rest of the world to make the most of AI, but could also highlight the disparity between FSIs who have not adopted the technology until now and those who have. In the latter example, greater pre-survey adoption by US respondents would register as lower overall support for this answer.

AI is also highly likely to factor into decisions of the 39 per cent of respondents who said they will continue relying on existing tools with incremental improvements. While this does not necessarily mean greater AI adoption, it suggests that many FSIs expect to modernise their existing fraud capabilities without completely replacing their current approach. A fifth (20 per cent) predict no significant change in strategy, indicating that a sizeable minority of FSIs remain cautious about making major changes to their fraud

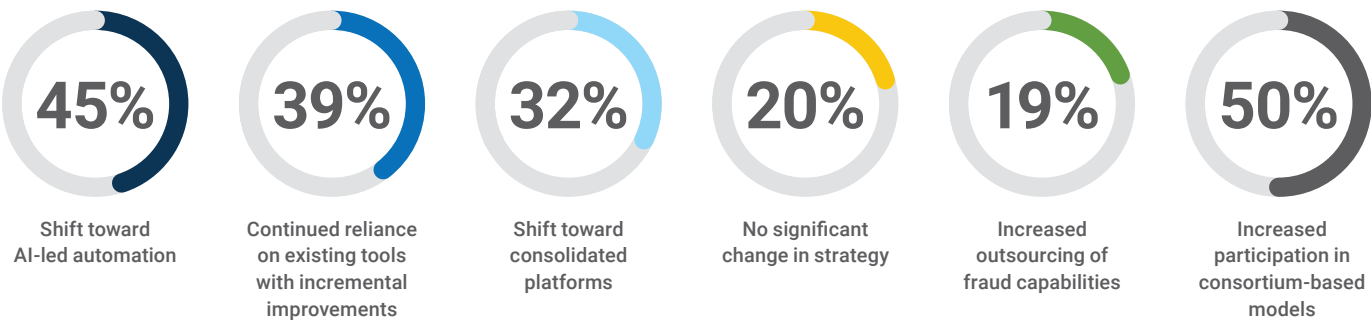
intelligence approach. This is broadly consistent with the more cautious attitudes towards AI and consortium participation seen elsewhere in the research.

Throughout the research, a sizable number of respondents made it clear that fraud data-sharing consortia and AI have tangible roles to play in the future of their fraud response. It is worth noting that respondents may also have interpreted the question through the lens of organisational necessity, rather than as a request for a projection based on their current aims and concerns. A chunk of respondents logged interest in both AI and consortia despite their potential risks, indicating that they expect to pursue both once they have dealt with factors such as regulatory uncertainty, budgetary constraints, or legacy tech barriers.

Where exemplar strategies are already clear, progression may be easier. This is hinted at by the 19 per cent of respondents who said they will pursue participation in consortium-based models over the period and an identical percentage who said they will outsource more of their fraud capabilities. In both cases, respondents indicate that some FSIs are happy to follow proven approaches that have resulted in demonstrably improved fraud intelligence by sectoral peers, whether that means joining a consortium or paying an established vendor to do more on their behalf, in place of more hands-on approaches such as internally managed AI deployment.

Why this matters: Fraud intelligence is evolving toward faster, more collaborative, and increasingly data-driven response models. The opportunity is to help financial institutions modernize while maintaining governance, trust, and operational control.

How is your organisation's fraud intelligence strategy expected to evolve over the next 24 months? (Select up to two options)



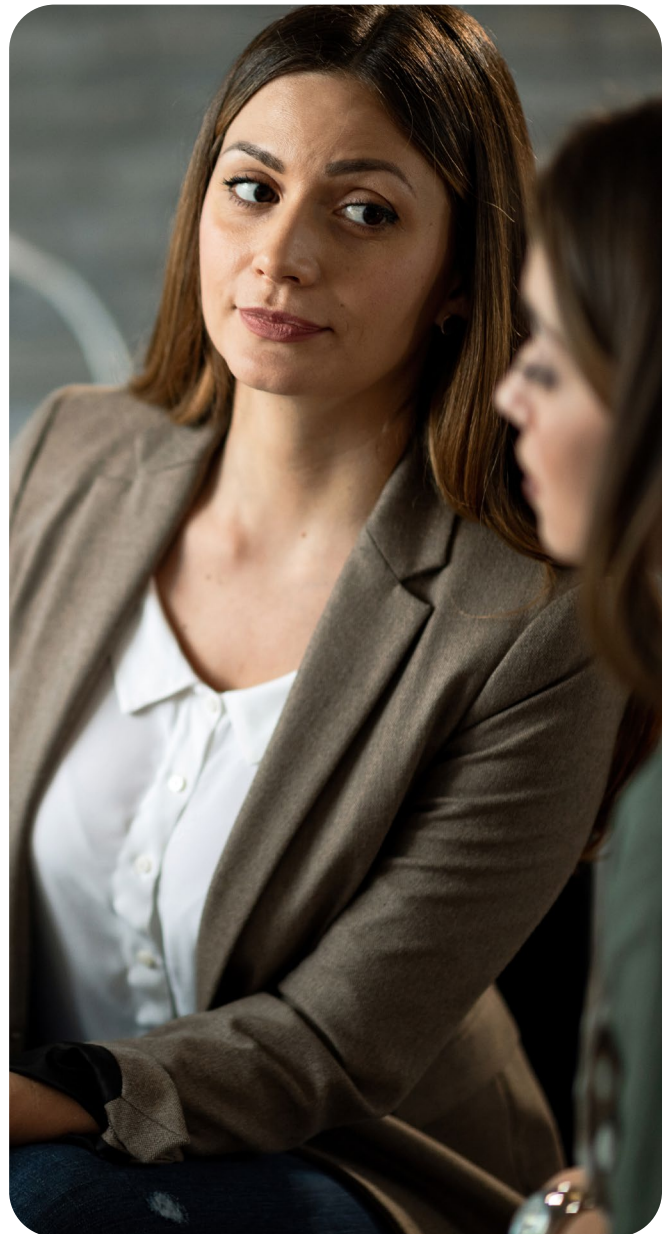
Conclusion

The survey findings point to a clear tension in the sector, with FSIs finding themselves at a crossroads over how best to tackle fraud. There is no doubt that leaders recognise the potential value of fraud data-sharing consortia, with respondents repeatedly identifying improved accuracy and speed in fraud recognition as key benefits of participation.

At the same time, the results indicate that regulatory and risk-related hurdles continue to deter FSIs from participating in fraud consortia and adopting the next generation of anti-fraud technologies. While few indicate they see little value in consortia or AI adoption whatsoever, concerns over data privacy, compliance, and trust in opaque AI models act as making leaders think twice about radically overhauling their fraud intelligence strategy. These are not necessarily the actions of naysayers, but leaders weighing the benefits of new approaches against their organisational needs and risk appetite. There are clear reasons for FSIs to consider how they can adopt new approaches to fighting fraud, particularly as threat actors increasingly use technology to scale and accelerate attacks.

Bridging this gap, and bringing the entire sector together, will require commitments to practices that retain the benefits of consortia while addressing their downsides. This includes robust data protection and anonymisation measures, as well as clearer legal guidance for how to participate in consortia without compromising their regulatory or confidentiality obligations. AI is a catalyst for change in financial services, and the responses indicate that this is both for better and for worse. The technology can drive faster, deeper, and more accurate responses to fraudulent activity, which dovetails with the benefits of fraud data-sharing consortia to provide improve how FSIs respond to threats. But AI is not only in the hands of the defenders. The technology is also behind evolving threats that are becoming a growing concern for FSIs and accelerating the pace at which they must adopt new tools.

FSIs that can strike the right balance, combining broader fraud intelligence with the capabilities unlocked by AI and advanced analytics, are likely to be better positioned to respond to this changing threat landscape. The research suggests that fraud response is becoming faster, more data-driven, and more collaborative, but that adoption will continue to be shaped by the need for effective governance, clear value and confidence in the technology.



FS*tech*

In collaboration with



Bottomline®