FStech In collaboration with Bottomline

The commercial payments fraud landscape: Threats, responses and strategic priorities

Introduction

Financial crimes affecting commercial payments are increasing in scale and sophistication. Institutions now face a wide spectrum of threats, including business email compromise, payment diversion schemes, synthetic identities, and attacks enabled by artificial intelligence. These risks are compounded by client behaviour, operational pressures, and legacy processes that create openings fraudsters can exploit.

Advances in email technology and AI have lowered the cost and effort required to launch convincing attacks. Fraudsters can now operate at speed and across multiple channels, combining automation with social engineering to target employees and clients with greater precision. As losses grow and attack methods evolve, the urgency for firms to strengthen fraud prevention measures has never been greater.

The consequences of failing to adapt are significant. Financial losses, reputational damage, and declining customer trust can weaken the resilience of institutions, especially those still relying on fragmented controls or outdated detection systems. Many organisations are recognising that traditional approaches cannot keep pace with attacks that shift rapidly and exploit behavioural, procedural, or technological gaps.

In response, institutions are increasingly adopting tools such as AI-based monitoring, behavioural analytics, and technologies designed to detect deepfakes, voice cloning, and other AI-generated impersonation techniques. Yet technology alone cannot mitigate the full range of risks. Effective defence also depends on staff who understand the signals of emerging fraud patterns and clients who know how and when to act on alerts. Training, communication, and process design play a central role in reducing opportunities for criminals to bypass controls.

A single measure cannot prevent every attempt. Stronger resilience requires coordinated detection capabilities, consistent employee education, rigorous investigative processes, and proactive client engagement. Without these elements working together, organisations risk being overtaken by threats that evolve faster than their defences.

To examine how financial institutions are responding to this environment, FStech and Bottomline surveyed 100 commercial payments professionals. This report presents the results, assessing how firms are adapting to today's threat landscape, the role of emerging technologies, and the level of preparedness for AI-driven fraud that is reshaping commercial payments.

Methodology

FStech and Bottomline surveyed 100 commercial payments professionals to learn more about the evolving threat landscape facing business banking clients, the effectiveness of current fraud prevention strategies, and the strategic priorities shaping institutional responses.

This research aims to benchmark industry practices, identify emerging challenges, and understand how financial institutions are adapting their commercial fraud frameworks to address increasingly sophisticated attacks.

Key findings:

Institutions are underinvesting in commercial fraud prevention.

More than half of respondents (56 per cent) say they invest less in commercial fraud controls because commercial clients typically bear the financial losses. This represents the most significant single finding in the survey and highlights a critical exposure across the sector.

Operational pressure is a major driver of risky client behaviour.

Half of respondents (50 per cent) report that clients override fraud alerts due to pressure from executives to complete transactions. Complex approval processes (43 per cent) and limited awareness of fraud risks (42 per cent) also contribute to overrides.

AI-enabled fraud is reshaping the threat landscape.

Automated vendor impersonation at scale is viewed as the most significant emerging AI threat (46 per cent), followed by machine-learning–based pattern mimicry (42 per cent) and AI-generated business correspondence (41 per cent). These risks reflect a rapid shift toward industrialised, AI-driven fraud operations.

Many institutions lack adequate tools to detect AI-based attacks.

Only 11 per cent consider themselves well-equipped with dedicated AI detection capabilities. A combined 35 per cent describe their stack as somewhat, poorly, or not equipped at all, while 21 per cent are still evaluating upgrades.

Leading investment priorities focus on collaboration and skills.

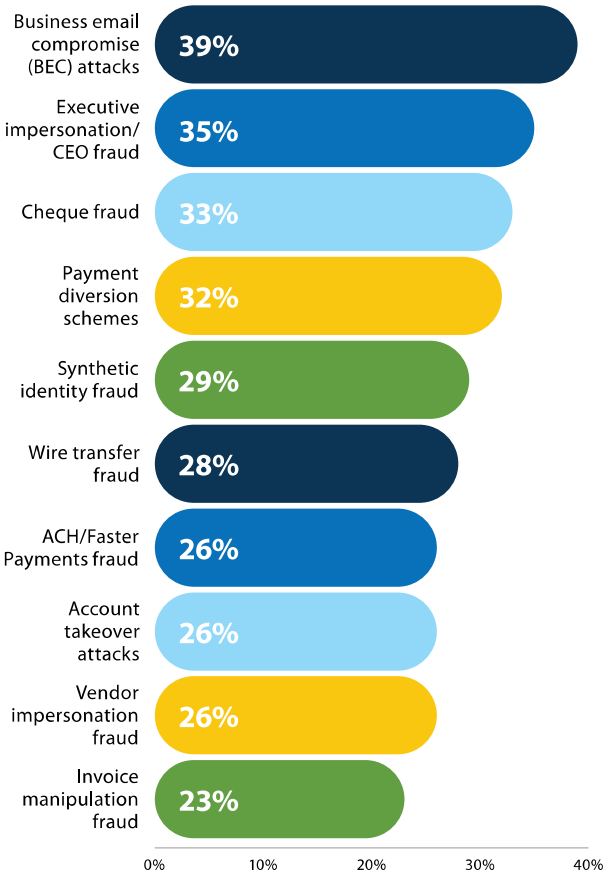
Institutions identify industry collaboration and intelligence sharing (41 per cent), specialist staff training (38 per cent), and client education (37 per cent) as key areas requiring additional investment, reflecting the importance of strengthening both human and collective defences.

Contents

1. Commercial payments fraud: an overview

The survey results show that fraud pressures are rising across multiple payment types, with no single category dominating the landscape. Business email compromise stands out as the most commonly cited threat, identified by 39 per cent of respondents as the fraud type that has increased most significantly over the past two years. This aligns with broader industry intelligence that continues to place BEC among the most damaging and persistent risks for commercial clients.

Which types of commercial payments fraud have increased most significantly at your institution over the past 24 months? (Select up to 3)



The operational impact of these attacks extends well beyond the immediate loss of funds. Only a minority of affected organisations recover most of the stolen money, and many face prolonged investigations, remediation work, and wider disruption to financial operations. The combination of financial loss, resource strain, and reputational harm makes BEC one of the most challenging forms of commercial fraud.

Other high-impact areas include executive impersonation or CEO fraud (35 per cent), cheque fraud (33 per cent), and payment diversion schemes (32 per cent). These categories illustrate how both traditional and digitally enabled methods continue to coexist, with criminals exploiting established processes as well as newer, technology-driven channels. Synthetic identity fraud (29 per cent), wire transfer fraud (28 per cent), ACH and Faster Payments fraud (26 per cent), and vendor impersonation (26 per cent) highlight the continued expansion of fraud activity across modern payment infrastructures.

Taken together, the results reflect a broad and fast-moving threat environment. Fraudsters are benefiting from inexpensive automation, convincing digital impersonation tools, and gaps created by fragmented or legacy detection systems. To counter this, organisations need coordinated defences that combine behavioural monitoring, secure payment networks, multi-factor authentication, and processes that limit human-error risk.

Cultural and procedural factors also shape exposure. Employees under pressure, inconsistent verification practices, and gaps in user training can neutralise otherwise strong controls. Addressing these behavioural risks is as important as deploying advanced technology. Regular training, awareness programmes, and clear escalation paths help ensure that staff approach unexpected or high-risk requests with appropriate caution.

Given the scale of the challenge, many institutions recognise the need for specialist partners and secure infrastructures that protect supplier credentials and restrict how payments can be initiated or amended. A multi-layered approach remains essential, combining modern monitoring tools with strong governance, well-trained teams, and resilient payment processes designed to prevent both internal and external compromises.

2. Why clients override fraud warnings

The survey findings indicate that overrides are influenced more by behavioural and operational pressures than by technological shortcomings. Executive pressure to complete transactions is the most common factor, cited by 50 per cent of respondents, showing how commercial urgency can lead clients to dismiss alerts even when controls are working as intended.

Complex approval processes contribute significantly, with 43 per cent reporting that slow or cumbersome workflows encourage users to bypass warnings in order to maintain business momentum. Limited understanding of fraud risks (42 per cent) and confidence in long-standing vendor relationships (38 per cent) further demonstrate how assumed familiarity or routine can reduce scrutiny of high-value transactions.

Limited fraud awareness training, also cited by 38 per cent, reinforces the importance of consistent and ongoing education. Users who do not understand why alerts trigger, or who are unclear about the relevance of specific risk indicators, are far more likely to override them. Urgent client deadlines, perceived inconvenience, and the belief that controls are overly cautious all add to the likelihood that warnings are ignored.

The findings highlight the need for institutions to address the human and procedural causes of overrides. Alerts must be clear, timely, and easy to interpret, reducing the cognitive load on users and helping them understand the significance of the warning. Streamlined approval workflows, particularly for high-risk scenarios, can reduce the temptation to bypass controls under pressure.

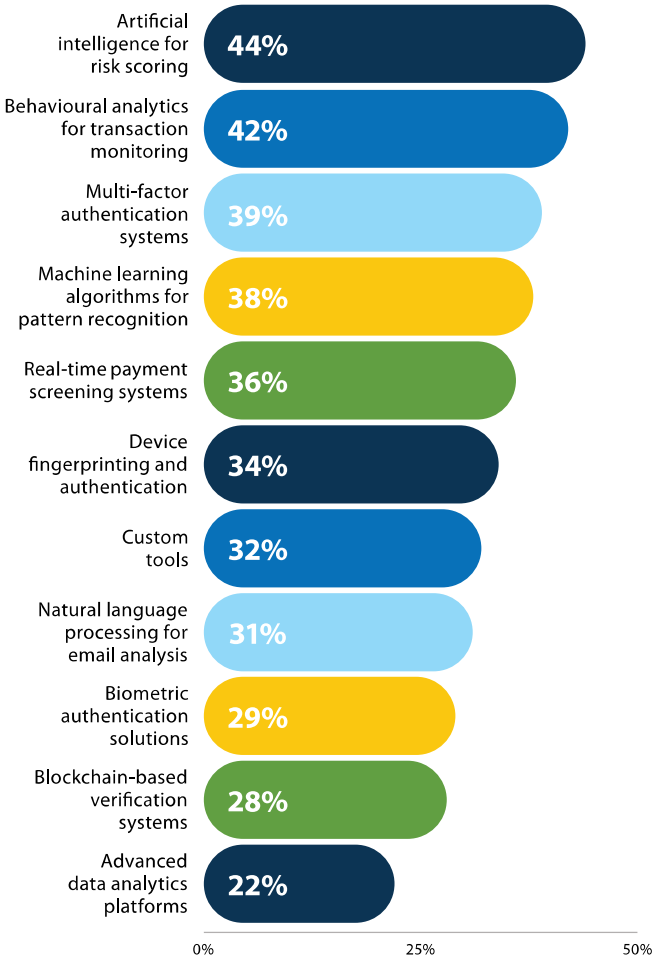
Automation and early-stage detection also play a role. Behaviour-based monitoring, real-time analytics, and proactive flags at the point of entry can identify anomalies before they reach the final approval stage, reducing both friction and reliance on manual checks. By redesigning processes and reinforcing staff awareness, institutions can reduce the frequency of overrides without disrupting legitimate business activity.

Which factors most commonly lead commercial clients to override fraud warnings? (Select up to 3)

3. Advanced technology in fraud detection

The survey demonstrates a broad uptake of advanced technologies across institutions, reflecting a clear shift toward more adaptive and analytics-driven fraud prevention. Artificial intelligence for risk scoring leads adoption at 44 per cent, closely followed by behavioural analytics at 42 per cent. These tools support earlier detection of unusual activity by identifying patterns that differ from established behaviour, rather than relying solely on static thresholds.

Which advanced technologies has your institution deployed specifically for commercial fraud detection? (Select all that apply)



Multi-factor authentication (39 per cent) and machine-learning models for pattern recognition (38 per cent) remain central components of modern fraud frameworks. These technologies provide layered protection that can identify complex threats and adapt to the evolving tactics of fraud actors, particularly as criminals use AI to mimic legitimate transaction patterns.

Real-time payment screening (36 per cent), device fingerprinting (34 per cent), and the development of custom tools (32 per cent) reflect ongoing investment in capabilities that can operate at speed across diverse payment channels. Natural language processing for email analysis (31 per cent), biometric authentication (29 per cent), and blockchain-based verification (28 per cent) show that institutions are experimenting with specialised solutions that address specific attack vectors, including email compromise, account takeover, and document manipulation.

While these technologies provide strong improvements, they also introduce operational challenges. Fragmented or siloed detection tools can leave blind spots across channels, particularly if data and alerts are not integrated into a unified investigative workflow. Institutions with legacy infrastructure face additional obstacles, as older systems may not support real-time analytics or behavioural modelling.

Effective use of advanced technology requires both coherence and governance. Tools must operate together across channels, and investigators need clear visibility of alerts, cases, and behavioural histories. Institutions also need tuning capabilities that allow them to balance sensitivity and operational impact, reducing false positives without weakening protection. Without these elements in place, even sophisticated tools can struggle to detect high-risk activity at the pace required.

4. Emerging AI-powered fraud threats

The survey highlights a clear shift toward industrialised, AI-enabled attacks that span multiple communication channels and payment processes. Nearly half of respondents (46 per cent) identified automated vendor impersonation at scale as the most significant emerging threat. This reflects growing concern that fraudsters can now use automation and generative tools to mimic supplier communications, initiate fraudulent payment requests, and exploit gaps in accounts payable workflows with far greater speed and volume than before.

Machine-learning–driven transaction pattern mimicry (42 per cent) and AI-generated phishing emails (41 per cent) further illustrate how attackers are using advanced models to replicate legitimate behaviour and communication styles. These methods allow fraudulent activity to blend into normal transaction flows, making it harder for traditional rules-based systems to detect anomalies in time.

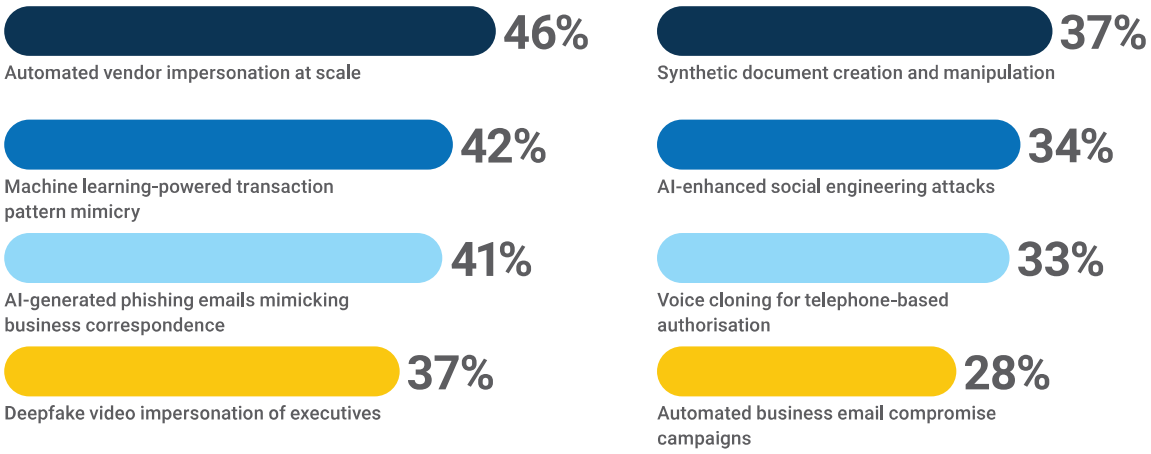
Deepfake video impersonation and synthetic document creation, each cited by 37 per cent of respondents, point to a maturing threat environment in which fraudsters can fabricate identities and supporting evidence with increasing credibility. These techniques raise the stakes for high-value transfers, onboarding processes, and executive-level authorisation requests, where visual verification or document checks have historically played a key role.

Respondents also noted the growing use of voice cloning (33 per cent) and AI-enhanced social engineering (34 per cent). These tools allow attackers to replicate executive voices, create convincing phone-based authorisation attempts, and manipulate staff under time pressure. In many cases, the goal is not a perfect imitation but one that is convincing enough to escape scrutiny during busy periods or at moments when staff expect to receive urgent instructions.

The breadth of these responses shows that institutions are now dealing with a multi-channel, AI-driven fraud ecosystem. Attackers can combine email, voice, documents, and transactional behaviour to build credible narratives that bypass legacy verification steps. The findings reinforce the need for layered defences that incorporate behavioural analysis, continuous identity verification, and real-time monitoring capable of detecting activity that diverges from expected user patterns even when surface-level signals appear legitimate.

This environment demands a shift in mindset. Traditional controls designed around static rules or post-event review cannot keep pace with attacks executed at machine speed. Institutions need tools that analyse context, behaviour, and environmental signals, supported by teams trained to recognise and respond to the early indicators of AI-enabled social engineering. Without these capabilities, organisations risk being overrun by highly scalable threats that exploit human, procedural, and technological weak points simultaneously.

Which AI-powered fraud techniques do you consider the most significant emerging threats to commercial payments? (Select up to 3)



5. Firm readiness for AI fraud

The survey reveals a significant readiness gap as institutions confront increasingly advanced fraud techniques. Only 11 per cent of respondents believe they are very well equipped with dedicated AI detection capabilities, and although a further 25 per cent consider themselves moderately equipped, the majority report limited or inconsistent preparedness. Many still rely heavily on traditional methods that lack the speed or adaptability needed to counter AI-generated attacks.

A combined 35 per cent describe their technology stacks as somewhat, poorly, or not equipped at all. This indicates that a considerable proportion of institutions operate without the monitoring depth or behavioural analytics necessary to detect deepfakes, voice cloning, synthetic identities, or automated phishing campaigns. Another 9 per cent are unsure of their capabilities, which suggests gaps in governance, visibility, and internal assessment processes.

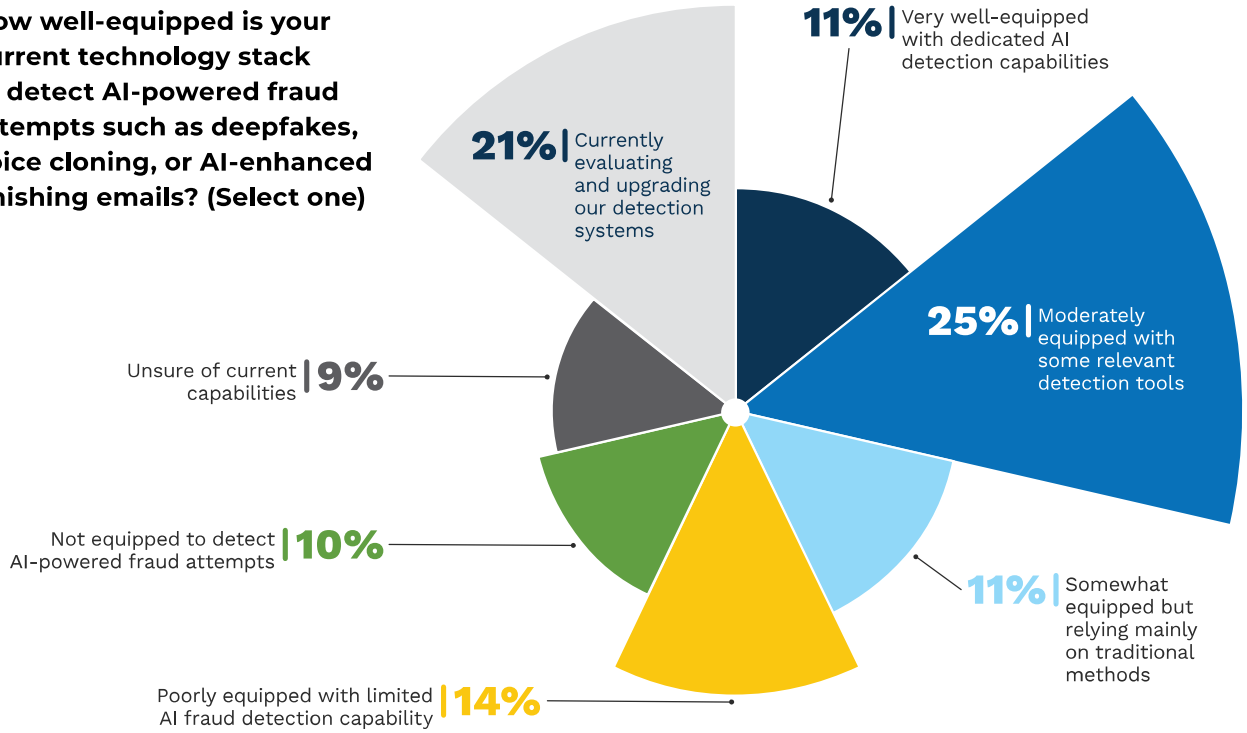
The 21 per cent of respondents who are evaluating or upgrading their systems point to a recognition that current controls are not sufficient. However, this also implies that many institutions are in transitional phases where defences may be fragmented or partially deployed, leaving blind spots that can be exploited by attackers who move quickly between channels.

This readiness challenge is amplified by the nature of modern fraud. AI-driven attacks often begin after login, when traditional authentication has already taken place. Fraudsters may use compromised credentials, session hijacking, or behavioural mimicry to operate within an authenticated environment. Detection therefore requires tools that go beyond identity checks and focus on continuous behavioural analysis, environmental context, and deviations from established user profiles.

Stronger governance frameworks are also needed. As institutions adopt more advanced detection capabilities, they must ensure effective model validation, structured oversight, and clear accountability for how AI tools are deployed and monitored. Weak governance can create new vulnerabilities, whether through false positives that overwhelm investigators or false negatives that allow sophisticated attacks to pass unnoticed.

The results show that institutions understand the scale of the challenge but have not yet achieved the level of readiness required to confront industrialised, AI-enabled fraud. Closing this gap demands investment in advanced analytics, unified detection platforms, and investigative tools that give teams a full view of cross-channel activity. Without this foundation, organisations risk falling behind at a time when attackers are expanding their capabilities at pace.

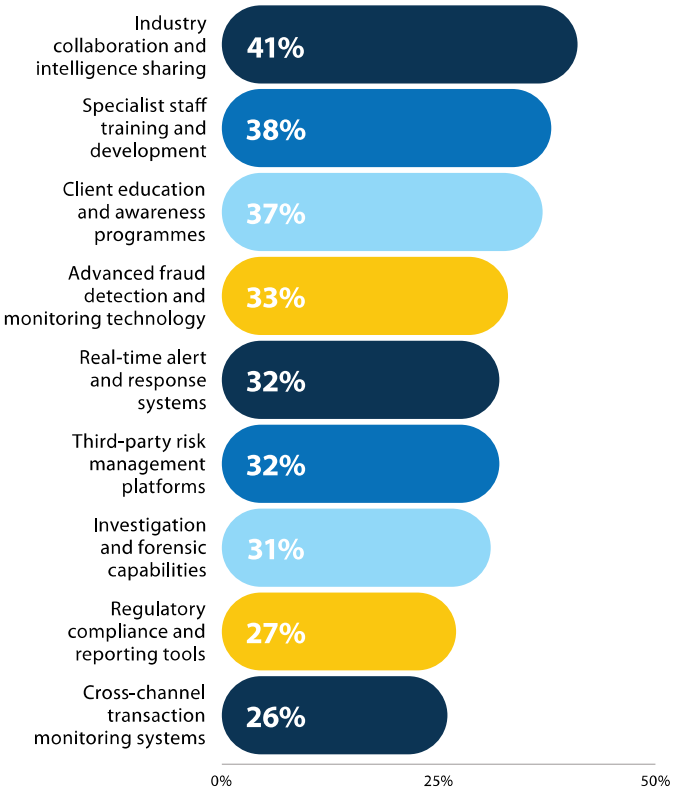
How well-equipped is your current technology stack to detect AI-powered fraud attempts such as deepfakes, voice cloning, or AI-enhanced phishing emails? (Select one)



6. Priority areas for fraud investment

The survey responses point to a broad set of investment needs, reflecting the complexity of commercial fraud and the varied pressures institutions face. Industry collaboration and intelligence sharing stand out as the top priority, cited by 41 per cent of respondents. This underscores the recognition that no single institution can match the scale, speed, or adaptability of today's fraud networks without support from peers and industry bodies. Shared intelligence helps close visibility gaps, align responses, and strengthen sector-wide resilience.

Which areas require the most additional investment to strengthen your commercial fraud capabilities? (Select up to 3)



Specialist staff training (38 per cent) and client education programmes (37 per cent) also rank highly. These responses highlight persistent vulnerabilities in human behaviour, both within institutions and among clients, and the importance of equipping teams with up-to-date knowledge about AI-enabled attacks, social engineering techniques, and evolving threat patterns. Training must be ongoing rather than episodic, ensuring that staff can recognise anomalies even as fraud tactics shift.

Technology-focused priorities also feature prominently. One third of institutions identify advanced detection and monitoring technology (33 per cent), and similar proportions point to real-time alert and response systems (32 per cent) and third-party risk management platforms (32 per cent). These areas address the need for faster detection, coordinated response, and greater oversight of suppliers and partners who may be targeted as entry points for fraud campaigns.

Investment in investigation and forensic capabilities (31 per cent) reinforces the importance of end-to-end resilience. Modern fraud often spans multiple systems and channels, requiring investigators to analyse behavioural histories, session data, user interactions, and cross-platform activity in a unified view. Without effective investigative tools, even strong detection capabilities can be undermined by delays or incomplete analysis.

Regulatory compliance and reporting tools (27 per cent) and cross-channel transaction monitoring (26 per cent) round out the key areas of focus. These responses reflect both regulatory expectations and operational realities. As payment volumes increase and fraud tactics diversify, institutions need systems that provide consistent oversight across ACH, wire, SWIFT, Faster Payments, and cheque channels. Fragmented monitoring increases the risk of blind spots that attackers can exploit.

Overall, the findings indicate that institutions see the need for balanced investment across people, technology, and shared intelligence. Strengthening any single component in isolation is unlikely to be enough. Effective defences require integrated systems, well-trained teams, collaborative networks, and investigative processes capable of responding at the speed and scale of modern fraud activity.

7. Impact of liability differences

The survey results show a clear imbalance between institutional responsibility and client exposure in commercial fraud.

More than half of respondents (56 per cent) say they invest less in commercial fraud prevention because losses typically fall on the client. This is the strongest single result in the entire survey and has direct implications for the level of protection commercial customers receive. It also suggests that many institutions continue to view commercial fraud primarily through a liability lens rather than as a strategic risk that affects operational resilience and customer confidence.

Half of respondents (50 per cent) report focusing more heavily on client education for the same reason, shifting responsibility toward customers who may lack the specialist knowledge, tools, or processes required to manage increasingly complex threats. While client education is essential, it cannot substitute for robust institutional controls, particularly as fraud methods grow more automated and better resourced.

A further 45 per cent encourage customers to obtain fraud insurance, which can mitigate financial impact but does not address the underlying vulnerabilities that enable attacks. Insurance also cannot compensate for the operational disruption, reputational harm, or regulatory exposure that often accompany a major fraud incident. Meanwhile, 41 per cent provide enhanced services to help clients manage their exposure, indicating a growing recognition that a more proactive approach is needed.

Interestingly, 40 per cent report maintaining consistent prevention standards regardless of liability, while 36 per cent adjust pricing or fees to reflect liability differences. These responses suggest a fragmented approach across the sector, where commercial fraud prevention strategies vary widely depending on internal risk appetite, customer expectations, and business model considerations.

The findings underline a structural tension. Commercial clients expect the same level of protection found in retail banking, but the allocation of losses places primary responsibility on them. 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 does the liability difference between commercial and retail fraud (where commercial clients typically bear losses) affect your fraud prevention approach? (Select up to 3)

8. Regulatory developments for fraud prevention

Respondents identified several regulatory developments that they believe would strengthen commercial fraud prevention across the industry. Standardised reporting requirements for commercial fraud data were cited by 43 per cent, making this the most widely supported regulatory measure. Consistent reporting structures would help institutions benchmark performance, improve transparency, and identify emerging trends earlier by increasing the comparability of data across the sector.

Clearer liability frameworks, highlighted by 41 per cent, reflect a need for more structured guidance on the responsibilities of each party in commercial fraud cases. Ambiguity in liability can delay incident response, hinder recovery efforts, and create uncertainty in strategic planning. Formalising these frameworks would allow institutions to design controls and processes with greater confidence and consistency.

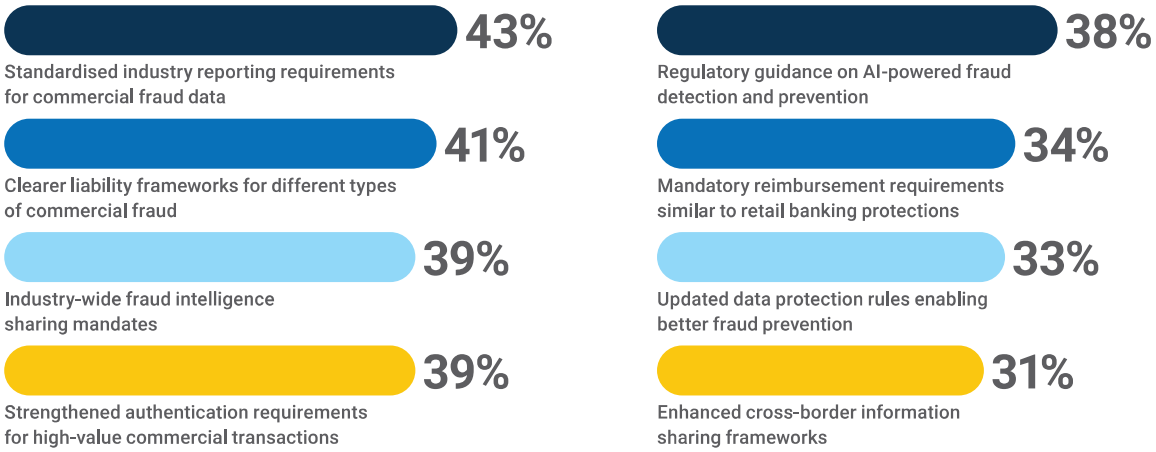
Industry-wide intelligence sharing mandates and strengthened authentication requirements, both cited by 39 per cent, point to areas where regulatory support could accelerate improvements already recognised as necessary by many institutions. Shared intelligence reduces blind spots and helps smaller institutions access insights normally available only to organisations with advanced analytics capabilities. Stronger authentication standards would raise the baseline for high-value and high-risk transactions, reducing opportunities for social engineering and unauthorised access.

Regulatory guidance on AI-powered fraud detection (38 per cent) was also identified as a priority. As institutions adopt more advanced analytics and monitoring tools, they face growing expectations around model governance, explainability, data quality, and validation. Clear regulatory expectations would help ensure that AI models are deployed safely and effectively, minimising unintended risk while improving detection quality.

Mandatory reimbursement requirements similar to retail protections (34 per cent) and updated data protection rules (33 per cent) highlight the ongoing balancing act between consumer protection, operational efficiency, and privacy considerations. Enhanced cross-border information sharing frameworks (31 per cent) reflect the reality that commercial fraud often spans multiple jurisdictions, requiring coordinated oversight that extends beyond domestic policies.

Together, these responses show that institutions see regulation not only as a compliance requirement but also as a mechanism for reducing industry-wide vulnerabilities. Consistent frameworks, shared intelligence, and clear expectations can help raise standards across the sector and reduce fragmentation in how commercial fraud is identified, reported, and managed.

Which regulatory developments would most effectively strengthen commercial fraud prevention across the industry? (Select up to 3)



9. Balancing security and payment speed

The survey results show how institutions navigate the tension between fraud prevention and commercial client expectations for rapid processing. Nearly half of respondents (44 per cent) allow clients to accept higher levels of risk in exchange for faster payments. This reflects practical business pressures but also introduces challenges, as increased throughput can create opportunities for fraudsters who rely on speed, urgency, and reduced scrutiny to bypass controls.

How do you balance fraud prevention requirements with commercial client demands for payment speed and convenience? (Select up to 3)

Risk-based authentication, cited by 42 per cent, is one of the primary methods institutions use to manage this tension. By adjusting verification requirements based on transaction profiles, risk scores, or behavioural patterns, institutions can apply strong checks where they are most needed while minimising friction for routine activity.

At the same time, 40 per cent report maintaining consistent security standards regardless of client preferences, recognising that relaxing controls can create systemic vulnerabilities that extend beyond individual transactions. This group prioritises baseline resilience even when clients request faster or more streamlined processes.

Technology also plays a central role. Thirty-seven per cent of respondents leverage tools that make security measures less intrusive, helping reduce friction without compromising protection. Similarly, 36 per cent regularly review and optimise processes to streamline workflows, address bottlenecks, and reduce unnecessary manual checks.

Tiered service levels, offered by 35 per cent of respondents, provide clients with choices that balance speed and security. This approach recognises the diverse risk appetites across commercial clients and enables institutions to tailor controls without weakening core protections.

Client education remains a critical factor. Thirty-two per cent provide extensive education to improve client understanding of why controls are necessary, and another 32 per cent use client risk scoring to calibrate measures for different segments. These initiatives help reduce conflict between operational needs and fraud prevention by aligning expectations and encouraging clients to participate in safeguarding their own payment processes.

These responses show that balancing fraud prevention with payment speed requires a mix of adaptable authentication, efficient processes, client engagement, and carefully structured service models. Institutions that rely too heavily on speed at the expense of security risk exposing themselves and their clients to significant losses, while those that impose rigid controls without flexibility may struggle to meet customer expectations. The most effective strategies integrate risk-based approaches that align security measures with the actual threat environment.

10. Key external influences on fraud strategy

The survey results show that institutions expect a broad set of external pressures to shape their commercial fraud strategies over the next two years. Industry collaboration and best practice sharing were cited by 42 per cent of respondents, reflecting the recognition that fraud has become a networked threat. Attackers often target multiple institutions and their clients simultaneously, making shared intelligence and coordinated responses essential for effective defence.

Resource constraints and budget pressures, cited by 40 per cent, continue to play a significant role in determining the scope and pace of investment. Institutions must balance the need for advanced detection technology, skilled staff, and resilient infrastructures against the financial realities of operating in competitive markets. These constraints can lead to difficult prioritisation decisions, especially when fraud losses do not directly affect the institution due to liability structures in commercial banking.

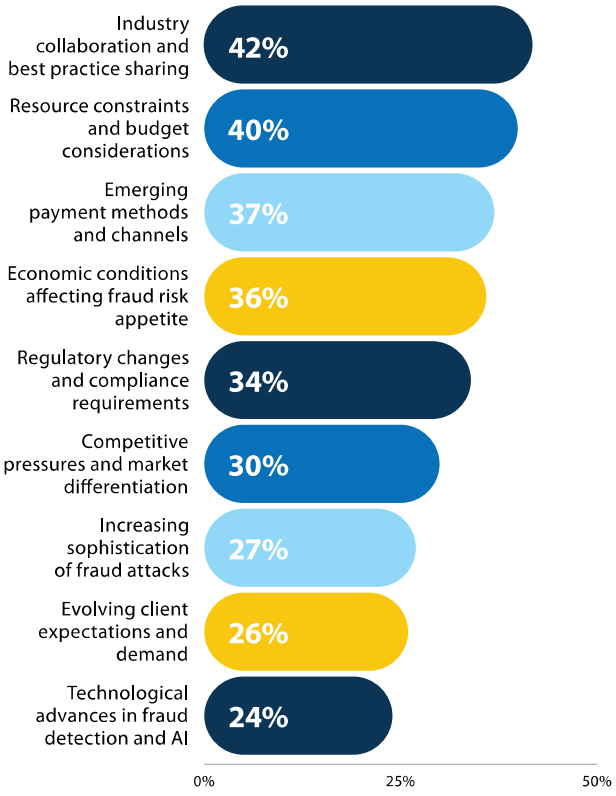
Emerging payment methods and channels (37 per cent) introduce additional challenges, as new pathways for transactions create fresh opportunities for fraud. Real-time payments, cross-border platforms, and digital trade finance solutions bring operational efficiencies but expand the attack surface. Thirty-six per cent highlight the impact of economic conditions, which can influence risk appetite, client behaviour, and fraud activity. Periods of financial strain often correlate with increased fraud attempts as both external actors and internal pressures escalate.

Regulatory changes (34 per cent) remain a significant influence, particularly as regulators refine expectations around AI governance, authentication standards, and industry reporting. Competitive pressures (30 per cent) also shape strategy, as institutions aim to differentiate themselves through enhanced security or faster payment experiences while maintaining strong defences.

The increasing sophistication of fraud attacks, cited by 27 per cent, reinforces the need for continuous adaptation. As generative AI, automation, and deep behavioural mimicry become more common, institutions must anticipate and respond to threats that evolve at greater speed and scale. Client expectations and demand (26 per cent) further influence how firms design controls, as commercial customers seek faster processes, more flexibility, and seamless interactions without compromising safety. Technological advances in fraud detection and AI (24 per cent) round out the list, demonstrating that innovation itself is both an enabler and a driver of strategic change.

Overall, the responses suggest that institutions operate within a complex ecosystem where technology, regulation, competition, and economic pressures intersect. Effective strategies must account for multiple external forces that can shift quickly and introduce new forms of risk, requiring flexible, data-driven, and collaborative approaches to commercial fraud prevention.

Which external factors will most influence your commercial fraud strategy over the next two years? (Select up to 3)



Conclusion

The survey findings reveal a commercial payments fraud landscape that is expanding in complexity and intensity. Respondents report that traditional threats such as business email compromise, executive impersonation, cheque fraud, and payment diversion schemes continue to grow, while AI-enabled techniques are emerging at pace. Automated impersonation, transaction pattern mimicry, and synthetic media highlight how fraud has evolved from isolated incidents to high-volume, technology-driven operations.

Despite these developments, the results show that many institutions remain insufficiently equipped to detect and respond to advanced attacks. Only 11 per cent consider themselves very well prepared for AI-enabled fraud, and a significant proportion rely on traditional methods that do not offer the speed or analytical depth required. This gap is compounded by operational pressures that lead clients to override alerts, often because of executive demands, complex processes, or limited awareness of fraud risks.

On the positive side, institutions are adopting a wider range of advanced technologies. AI-driven risk scoring, behavioural analytics, machine-learning models, and real-time payment screening are becoming more common, indicating a shift toward proactive and adaptive detection. However, gaps remain, particularly where legacy systems limit integration, cross-channel visibility, or the ability to analyse behavioural signals in real time.

The survey also highlights the importance of human readiness. Specialist staff training, ongoing client education, and streamlined processes are central to reducing vulnerabilities created by behavioural and procedural factors. Fraud prevention increasingly depends on informed decision-making at every stage of the payment journey, from initial request to final approval.

External influences will continue to shape institutional strategies. Industry collaboration, regulatory developments, emerging payment methods, and economic conditions all exert significant pressure on how organisations prioritise resources and design controls. Respondents also emphasise the need for clearer liability frameworks and standardised reporting, reflecting a call for consistency across the sector.

Commercial fraud carries substantial financial, operational, and reputational risks. Institutions cannot rely solely on client liability or reactive controls. A more resilient approach requires integrated technology, coordinated intelligence, skilled teams, and governance structures that support rapid detection and response. By adopting a balanced and intelligence-led strategy, institutions can reduce exposure, strengthen client trust, and meet the demands of an environment where fraud is increasingly industrialised and technologically advanced.

FSTech In collaboration with Bottomline®