NICE Actimize

Finextra

Survey report by Finextra Research
June 2026

The European Fraud Insights Report 2026

Contents

01 Foreword

Joe Bristow,
Product Director & Fraud SME, NICE Actimize

Across Europe, fraud has evolved from being managed primarily as a financial risk into something far broader — a challenge that cuts across customer trust, operational resilience, and how banks differentiate themselves in an increasingly competitive market.

Drawing on insights from 203 European fraud leaders, this report sets the scene for the fight against fraud in 2026, where the threat landscape is simultaneously broadening and accelerating.

Banks must continue to defend against established fraud typologies while contending with a new generation of threats. The industrialisation of fraud through Fraud-as-a-Service is lowering the barrier to entry for less-skilled actors, and generative AI is enabling scams that are more personalised, convincing, and harder to detect than anything the industry has faced before.

Concern around AI-initiated payment fraud is growing particularly quickly, and the trajectory is one Europe is watching closely. Yet for many institutions, the pace of modernisation is being held back by data fragmentation and organisational silos that make a coordinated response harder than it should be, leaving many fraud leaders cautiously confident but few fully ready for what lies ahead.

Whilst priorities and maturity levels vary across DACH, Benelux, the UK, Nordics, CEE, and Southern Europe, an underlying direction of travel is shared — the banks that will be the most effective are those moving from reactive detection towards real-time authentication and monitoring, recognising that how well you prevent fraud is no longer just a risk metric, but a measure of how much your customers trust you.

As finalised compromise texts from the Council of the EU for both the Third Payment Services Directive (PSD3) and the Payment Services Regulation (PSR) have recently been published, the bar will be raised once again for fraud detection, and just as with PSD2, we expect to see further innovation and competition around customer experience and crucially customer trust.

02 Methodology

Finextra Research, in association with NICE Actimize, surveyed 203 fraud professionals within European banks. The survey responses were collected in March 2026 across DACH (including Germany, Austria, Switzerland), Benelux (including Belgium, the Netherlands, Luxembourg), the United Kingdom, Nordics (including Sweden, Denmark, Finland, Norway, Iceland), CEE (including France, Poland, Czech Republic, Hungary, Romania, Bulgaria, Belarus, Slovakia, Estonia, Latvia, Lithuania), and Southern Europe (including Spain, Italy, Portugal, Greece, Malta).

Our outreach ranged from C-level to senior managers across retail banks, commercial/corporate banks, investment banks, private banks, development banks, and digital/challenger banks. Respondents spanned across departments including fraud risk management, fraud technology & analytics, fraud & financial crime, fraud operations, fraud strategy & policy, and fraud product.

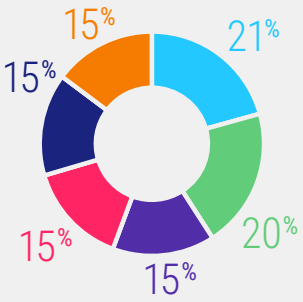
The survey combined quantitative data through self-administered questionnaires, with expert commentary from Santander UK, Banque de France, Klarna, and Lloyds Banking Group to give depth to the findings.

The full sample breakdowns by region, bank type, department, role level are shown below.

All survey responses were conducted on a confidential basis.

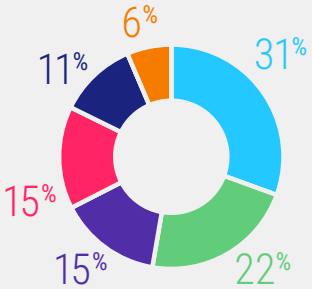
DEMOGRAPHIC SPLITS

Region



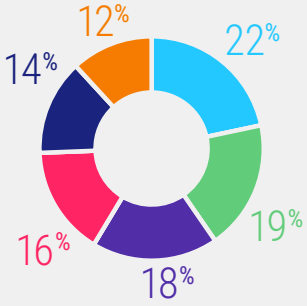
- DACH
- Benelux
- UK
- Nordics
- CEE
- Southern Europe

Bank type



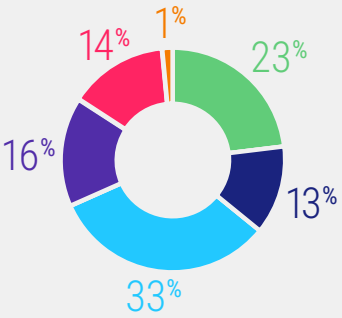
- Retail bank
- Commercial/ Corporate Bank
- Investment Bank
- Private Bank
- Development Bank
- Digital/Challenger Bank

Department



- Fraud risk management
- Fraud technology & analytics
- Fraud & financial crime
- Fraud operations
- Fraud strategy & policy
- Fraud product

Role level



- C-level
- Executive vice president or Senior vice president
- Vice president
- Senior director
- Director
- Senior manager

Figures are rounded to the nearest whole percentage.

03 Executive insights

01 Fraud risk is becoming systemic and AI driven

Fraud is no longer isolated to specific transaction types but embedded across the wider payments ecosystem. Digital banking growth, Fraud-as-a-Service (FaaS), and AI enabled tooling are increasing the scale, speed, and sophistication of attacks across Account Takeover (ATO), Authorised Push Payment (APP) fraud, synthetic identities, and AI initiated payment fraud. Nearly half (47%) of UK banks expect significant growth in AI initiated payment fraud, highlighting how quickly banks expect agentic-driven fraud to increase.

02 Trust erosion is now the primary cost of fraud

Customer attrition or erosion of trust now ranks ahead of direct financial losses as the most significant fraud impact. This shift reflects growing sensitivity around customer confidence in an increasingly competitive banking landscape, where switching providers has become easier and digital first challengers continue to reshape customer expectations.

03 AI is becoming central to fraud defence strategies

Only 2% of banks remain fully rules-based, most have either deployed or are piloting machine learning and generative AI. Customer-facing fraud prevention tools (including real-time warnings and scam intervention messages), are the most widely adopted use case, leveraged by nearly half of European banks (49%).

04 Hybrid AI models dominate, but integration is the key constraint

As the fraud landscape grows in complexity, banks are preferring to base their fraud strategies on multi-layered frameworks, with 38% leaning towards a hybrid approach, building certain capabilities in-house while outsourcing others to specialised vendors. When it comes to expanding AI adoption across fraud prevention, the greatest barrier is the complexity of integration with existing fraud platforms).

05 Human touchpoints as a critical control

Despite rapid AI adoption, the importance of keeping a human-in-the-loop remains. Fraud controls involving human intervention (via fraud specialists in bank contact centres) rank as the most effective fraud prevention controls in a bank. As signs of manipulation are highlighted via human-to human conversations with fraud specialists in bank contact centres, who can then direct conversations to help to protect unsuspecting customers, this helps to prevent fraud before it's authorised. 43% of CEE respondents rate it as 'highly effective', reinforcing the importance of combining advanced detection methodologies with human touchpoints.

06 Real-time mule detection remains only semi-mature across Europe

Money mule activity continues to be difficult to detect in real-time, particularly where legitimate appearing synthetic identities are involved. Whilst linkage between onboarding data and payment activity is becoming more mature as banks strive to unify their data to create more holistic customer profiles, most still rely on batch-based or retrospective detection which will need to be uplifted in light of Europe's Payment Services Regulations.

07 Data fragmentation and organisational silos limit effectiveness

Despite 97% of banks being at least 'somewhat confident', only 35% are 'very confident' in their fraud prevention capabilities in the near future. Data quality or data access limitations are the key roadblocks to improving fraud prevention capabilities, followed by organisational silos as well as a lack of skilled fraud technology talent. Considering fragmentation remains a challenge, four out of five European banks are actively planning or already executing the consolidation of multiple fraud risk engines into a unified platform.

08 The next phase of fraud investment

Over the next one to two years, the primary fraud prevention planned investment areas are AI and machine learning detection capabilities, money mule detection and interdiction, and fraud operations efficiency — each cited by 35% of European banks. Although AI investment is a consistent priority across regions, regional differences are emerging around areas such as real-time payment fraud controls, regulatory compliance, and customer education initiatives.

04 Where are banks seeing the greatest fraud pressure?

Fraud continues to evolve in scale and sophistication as digital payments expand and new technologies reshape the financial ecosystem. Financial institutions are facing increasing pressure to detect and prevent a wide range of fraud types while maintaining seamless customer experiences and meeting regulatory expectations. At the same time, fraud is no longer viewed solely as a financial issue, with growing concern around customer trust, operational resilience, regulatory pressure, and reputational impact.

To understand how banks are responding to these changes, our survey results begin with a baseline view on how specific fraud attacks have changed over the past 12 months, before assessing how fraud patterns are expected to evolve over the next three years, where concern is increasing across payment types, and the wider business impacts fraud is creating beyond financial loss.

Banks are facing simultaneous escalations across the threat landscape, with all fraud attacks scoring a weighted average of 3.94 and above out of 5, signalling a structurally elevated and broadly distributed risk environment.

TOTAL RESPONSE

How have fraud attacks (overall and specific types) against your institution changed over the past 12 months?

Ranked on a scale of 1 to 5	1 - No meaningful advancements/ impact	2	3	4	5 - Critical threat advancements/ impacts (poses a significant risk to operations)	Rank[1]	Score[2]
Account Takeover (ATO)	2%	10%	20%	44%	24%	1	4.24
New Account Fraud / Synthetic Identity	4%	8%	26%	38%	23%	2	4.14
Card fraud	3%	9%	27%	37%	23%	2	4.14
Authorised Push Payment (APP) fraud / Scams	3%	12%	27%	34%	25%	3	4.13
Overall fraud attacks	2%	12%	29%	34%	23%	4	4.09
Internal / Employee fraud	0%	16%	27%	37%	20%	5	4.02
Card-not-present fraud	6%	11%	24%	38%	21%	6	3.99
Money Mule activity (inbound and outbound)	3%	8%	24%	51%	14%	7	3.94

[1] based on weighted average order. [2] weighted average score to 2dp

0% 60%

04 Where are banks seeing the greatest fraud pressure?

The rise of FaaS (fraud as a service) is accelerating this trend by industrialising sophisticated attack techniques and lowering barriers to entry for less-skilled actors. This shift is materially increasing the scale, speed, and accessibility for fraud attacks, while AI is further accelerating the automation and sophistication of malicious activity across the financial ecosystem.

DACH reports the greatest high-end scores in Account Takeover (33% report 'critical threat advancements/impacts'), 9 percentage points above the European average.

Within this broader landscape, Account Takeover (ATO) leads as the most critical pressure point. The findings reinforce that as digital banking grows, ATO attacks increase in sophistication, making advanced authentication and continuous monitoring essential.

Chris Ainsley, head of fraud risk management at Santander UK, explains:

> *"The compromise of data is often the precursor to ATO, but the real issue lies in the gaps that criminals can exploit once they have that data. Organisations must be able to ensure that compromised data has minimal fraudulent value, regardless of its source. This requires a focus on protecting all high-risk operations and entry points across channels using dynamic controls that are resistant to social engineering. Layering behavioural detection on top of these controls is essential."*

Concern around new account fraud/synthetic identities is continuing to grow, signalling the next phase of AI-enabled financial crime.

Tom Martin, business platform lead - economic crime prevention at Lloyds Banking Group, comments:

> *"We're seeing fraud become hyper-personalised and industrialised at the same time. Generative AI enables highly tailored scams at scale; deepfake voice, synthetic identities, and real-time social engineering that adapts mid-conversation."*

This rise of synthetic identities presents a significant challenge, as even advanced detection tools can struggle to identify fraudulent profiles during onboarding. The survey results reflect that there is a broad industry expectation that their use in scams will only continue to increase.

Ainsley expands:

> *"The industrialisation of fraud is accelerating, as generative AI enables low-skill actors to execute high-quality scams at scale, including phishing campaigns, social engineering attacks, and the creation of convincing fake documents. At the same time, hyper-personalisation is becoming a defining feature of modern fraud. AI models can be used to scrape, collate, and even synthesise personal data, which in some regions can be particularly damaging. This allows fraudsters to create highly convincing, context-aware scams, such as those referencing real transactions or personal relationships, marking a significant shift from more generic, historically common attack methods."*

Scores for card fraud and Authorised Push Payment (APP) scams emphasise ongoing vulnerabilities across the full customer lifecycle as banks digitise rapidly. At the same time, banks are reporting increased attention on internal and employee fraud, highlighting the need for banks to strengthen both internal controls alongside customer-facing defences to safeguard trust and efficiency.

Collectively, these trends point to a fraud landscape growing significantly in both scope and complexity. The breadth and convergence of today's risks require a more integrated response, as this fundamentally differs from prioritising against one top risk, the need for a platform-based approach, rather than relying on isolated point solutions focused on individual attack types, will remain key.

Martin adds:

> *At Lloyds Banking Group, we've shifted focus from static rules and post-event investigation to real-time, AI-led prevention and intervention, embedding intelligence directly into customer journeys. The future belongs to banks building self-improving fraud systems that get smarter with every signal, every interaction, and every threat."*

The combination of AI-driven fraud, easier access to criminal tools, and the growth of digital banking will continue to add pressure on disconnected fraud controls already struggling to keep up with fast-changing attack patterns. The organisations best placed to respond will be those that treat fraud as an enterprise-wide resilience issue.

However, no bank can face escalating fraud by itself. To visualise how the wider industry can come together to more effectively address fraud vectors:

Alexandre Stervinou, director of cash and retail payments policy and oversight at the Banque de France, explains:

> *Let me take a concrete example on how banks can act together against fraud. The OSMP [the French Observatory for the Security of Payment Means] reported that remote card transactions were significantly more secure when using the 3-D Secure protocol, including for managing regulatory exemptions to Strong Customer Authentication (SCA) under PSD2. Thanks to a coordinated approach with banks, merchants, and card schemes, the OSMP has then recommended a systematic use of 3-D Secure for online transactions and is now actively supporting its use for telephone-ordered card transactions. The regulatory requirements on SCA, together with OSMP's recommendations, reduced the fraud rate of internet card transactions by 50% between 2018 and 2025. This action plan, conducted under OSMP's umbrella, has been very effective and can be a source of inspiration in other European countries."*

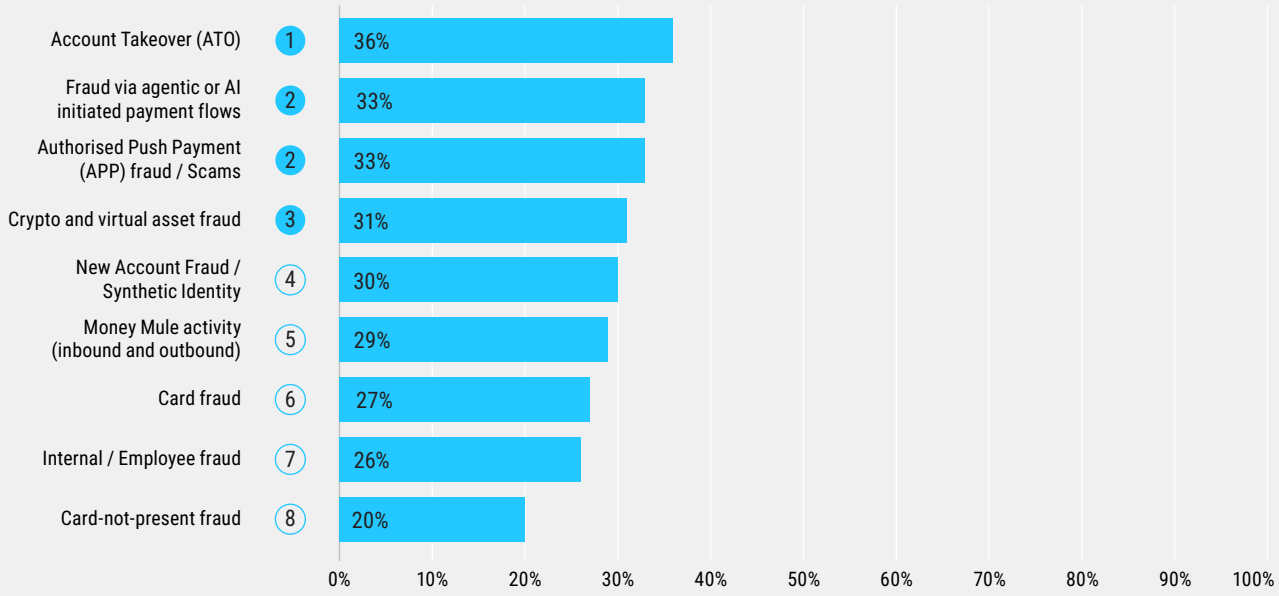
Emerging technologies and payment types necessitate stronger defences

Looking ahead, our survey results highlight how banks expect these pressures to intensify further over the next three years as digital payment innovation and increasingly accessible criminal tooling continues to reshape the threat landscape.

TOTAL RESPONSE

Which fraud types do you anticipate will grow most significantly over the next three years?

Select up to three options



Over the next three years, banks expect growth to continue across both established and emerging fraud types, led by Account Takeover (ATO) at 36%. Fraud via agentic or AI initiated payment flows follow closely at 33%, highlighting how quickly banks expect agentic-driven fraud to grow. Concern is particularly pronounced in the UK, reflecting both the pace of AI adoption across financial services, with **75% of UK financial services firms now using AI**, alongside growing awareness of its misuse by attackers.

Nearly half of respondents (47%) in the UK predict significant growth for AI initiated payment fraud, 14 percentage points above the European average.

While more traditional threats such as card and card-not-present fraud remain persistent, emerging areas such as crypto and virtual asset fraud are moving more into the mainstream, where controls and industry standards are still maturing. As new payment models, digital assets, and AI-enabled services become more widely adopted, fraudsters are quickly identifying opportunities to exploit gaps in onboarding and transaction monitoring processes. This is placing greater importance on real-time intelligence and cross-industry collaboration that can respond quickly as attack patterns evolve.

For banks, the challenge is managing a constantly expanding and increasingly interconnected threat landscape, in a world where fraud is evolving in step with technological change — and in some areas, faster than institutions are able to adapt their controls.

Ainsley explains:

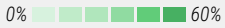
> *In reality, firms need to closely review the fraud types they are experiencing, assess these trends, and ensure they are capable of defending against 'good-enough' deepfakes and remote verification flows. They should also review fraud, financial crime, and identity controls to identify gaps, particularly where they may struggle to detect synthetic identities at onboarding due to fragmented signals across internal systems. Preventing criminals from exploiting these gaps requires a full assessment of cross-channel attack vectors, where fraud can span multiple entry points."*

TOTAL RESPONSE

How concerned are you about fraud risk associated with the following payment types?

Ranked on a scale of 1 to 4	1 - Very concerned	2 - Somewhat concerned	3 - Not concerned	4 - Not relevant to us	Rank[1]	Score[2]
SWIFT / High-value wire transfers	35%	49%	15%	1%	1	1.83
Central Bank Digital Currencies (CBDCs)	34%	49%	15%	2%	2	1.84
Faster / Instant payments (e.g. SEPA Instant, UK Faster Payments)	36%	44%	18%	1%	2	1.84
Card payments (card-not-present)	33%	50%	14%	3%	3	1.87
Mobile banking	32%	51%	16%	1%	4	1.88
Cryptocurrency and virtual asset flows	31%	52%	14%	3%	5	1.89
AI-initiated / Agentic commerce payments	30%	53%	14%	3%	6	1.90
Open Banking / Pay by Bank	34%	45%	19%	2%	6	1.90

[1] based on weighted average order. [2] weighted average score to 2dp



Concern around fraud risk remains consistently high across payment types, with every category scoring a weighted average of at least 1.83 out of 4, sitting within the 'very concerned' or 'somewhat concerned' range. This suggests that banks increasingly view fraud risk as embedded across the wider payments ecosystem, rather than concentrated in any single channel. The high concern scores further reflect the pace at which digital adoption is reshaping transaction environments and expanding potential attack surfaces.

For fraud risk associated with SWIFT/High-value wire transfers, Benelux reports the highest concern levels, with 39% of respondents reporting being 'very concerned'.

This broadening risk profile is increasing pressure on banks to strengthen visibility across the full payments lifecycle, improve coordination between fraud and payments teams, and invest in controls that can adapt quickly as customer behaviour and fraud tactics evolve. The challenge for leadership is no longer determining which payment type poses the greatest risk, but ensuring resilience across an increasingly diverse and continuously changing payments environment.

This complexity also means that fraud prevention measures need to span further than just financial institutions themselves. In France, for example:

Stervinou explains:

> *The OSMP has coordinated targeted actions with the telecommunication sector to address spoofing and smishing techniques, including the technical implementation of an authentication mechanism of phone numbers during calls, to halt the spoofing of bank phone numbers, and the protection against fraudulent SMS messages. New cooperation models with digital platforms and major technology players such as Google, Meta or Tik-Tok are currently under development, moving in the same direction."*

Top regional fraud concerns by payment types

DACH
Faster / Instant payments, Card payments (card-not-present) & Mobile banking (all 41% 'very concerned')

Benelux
AI-initiated / Agentic commerce payments (49% 'very concerned')

UK
Central Bank Digital Currencies (53% 'very concerned')

Nordics
Open Banking / Pay by Bank (30% 'very concerned')

CEE
Faster / Instant payments (60% 'very concerned')

Southern Europe
Card payments (card-not-present) (40% 'very concerned')

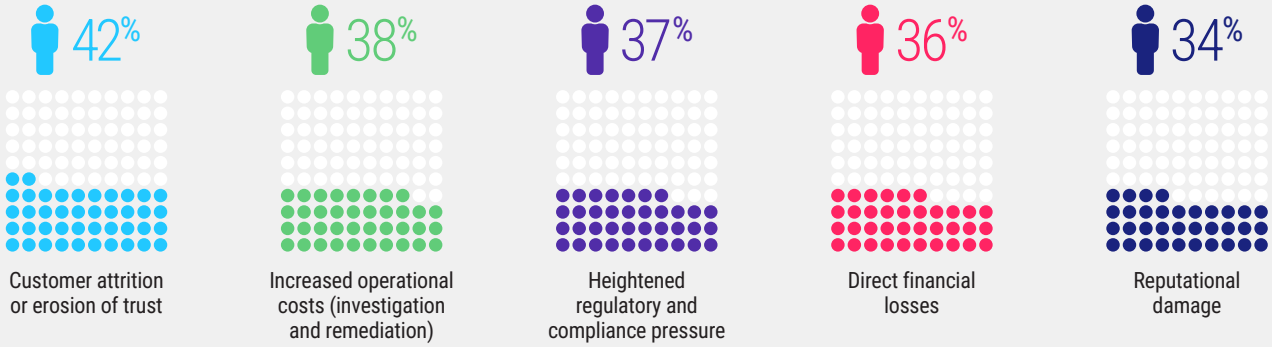
Trust and retention overtake financial losses as the primary fraud impact

As organisations respond to this rising fraud exposure, our survey results go on to highlight how banks are increasingly feeling the downstream impact not only through financial exposure, but through growing pressure on customer trust, operational resilience, and long-term retention.

TOTAL RESPONSE

What has been the most significant impact of fraud on your institution over the past 12 months?

Select up to two options



For the banks surveyed, the most significant impact of fraud over the past 12 months has been customer attrition or erosion of trust, cited by 42% of respondents — ranking ahead of financial losses and suggesting that modern fraud is a broader customer and business resilience issue rather than solely a financial risk.

The trend is particularly pronounced in the Nordics, where 60% of respondents identified 'customer attrition or erosion of trust' as the most significant impact of fraud, 18 percentage points above the European average.

Increased operational costs and heightened regulatory pressure follow, reflecting the growing burden associated with investigation, reimbursement, and compliance activity as fraud volumes and complexity continue to rise. Reputational damage scores highlight the growing sensitivity around customer confidence in an increasingly competitive banking environment, where switching providers has become easier and digital first challengers continue to reshape expectations. As fraud incidents become more visible and customer tolerance for disruption declines, maintaining trust is becoming as important for banks as preventing financial loss itself.

The findings point to the impact that fraud is extending beyond monetary losses. Banks are increasingly dealing with the combined effect of higher operational pressure, growing customer frustration, and greater reputational risk at the same time. This reinforces the need to strengthen fraud controls without creating unnecessary friction or adding further operational complexity. Banks that fail to strike this balance not only risk higher fraud exposure, but also the loss of both customers and competitive positioning in a market where trust is becoming a key differentiator.

05 How are European banks fighting fraud in 2026?

In light of these developments and the increasing pressure to detect and prevent an increasing number of fraud typologies, what do the operational capabilities of European banks look like in 2026?

As we investigated AI and machine learning maturity for organisations, our survey broadly differentiates between three stages of deployment: Rules-based detection only, piloting, and in production.

TOTAL RESPONSE

How would you describe your institution's current AI and machine learning maturity in fraud prevention?

Encouragingly, only 2% of banks are still relying on rules-based detection only, signalling near universal recognition that traditional approaches are insufficient against modern fraud threats. The pilot phase, remains common, with 22% of banks running machine learning pilots, and another 17% exploring or piloting generative AI in their fraud strategies.

The majority of European banks, however, are already in production. 29% of organisations are leveraging machine learning for fraud detection, and nearly one in three banks (31%) have deployed generative AI in fraud operations or customer-facing applications.

Two out of three UK banks are already in the production phase, the most advanced region across Europe.

Particularly in light of the rapid development of AI capabilities — for both good and bad actors — an organisation's AI roadmap for fraud prevention is crucial to prevent critical failure. As the development of AI models sharpens, financial institutions need to ensure their AI roadmaps keep pace.

Martin comments:

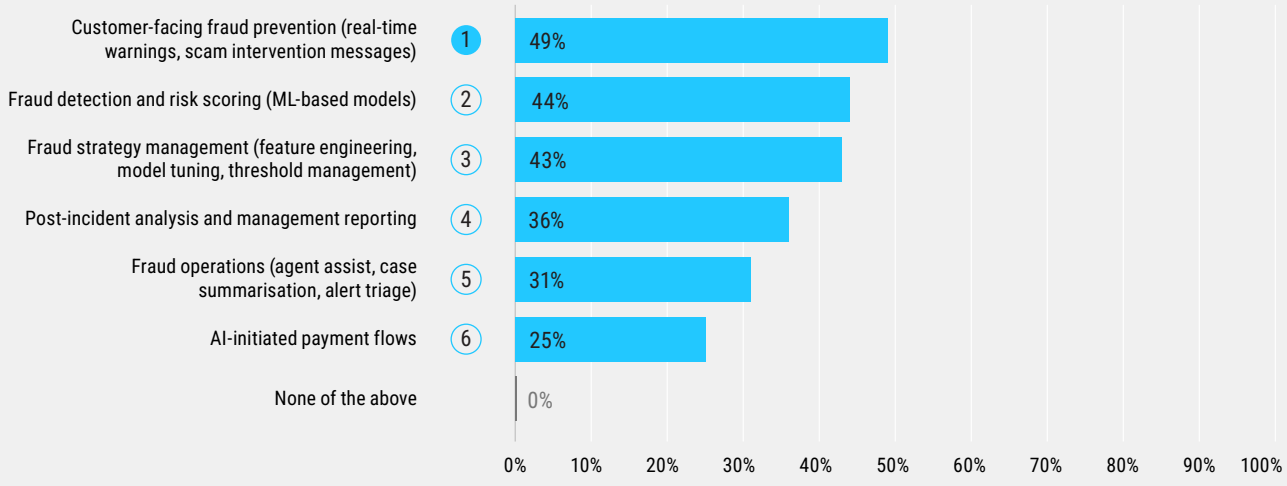
> *"What's noteworthy is not so much regional divergence in the threat itself, but the common directional challenge: fraud is becoming faster, more adaptive, and more blended across channels and typologies. Regardless of market, defensive strategies that rely on static rules or isolated controls struggle to keep pace."*

Digging more deeply into which areas AI is being integrated, our survey results find that banks are combining multiple advanced AI initiatives, re-emphasising Martin's point on the critical role of advanced and preventative fraud controls.

TOTAL RESPONSE

In which of the following areas is your institution currently using or evaluating AI?

Select all that apply



While ML-based fraud detection and risk scoring models are some of the longest standing use cases in fraud detection, in today's fraud landscape, customer-facing fraud prevention tooling has overtaken ML-based fraud detection models in terms of deployment.

Our survey found that customer-facing fraud prevention, such as real-time warnings and scam intervention, is currently being leveraged by nearly half of European banks (49%). ML-based fraud detection and risk scoring models follow (44%), ahead of fraud strategy management (43%).

Ainsley explains, particularly as banks are facing growing numbers of ATO fraud:

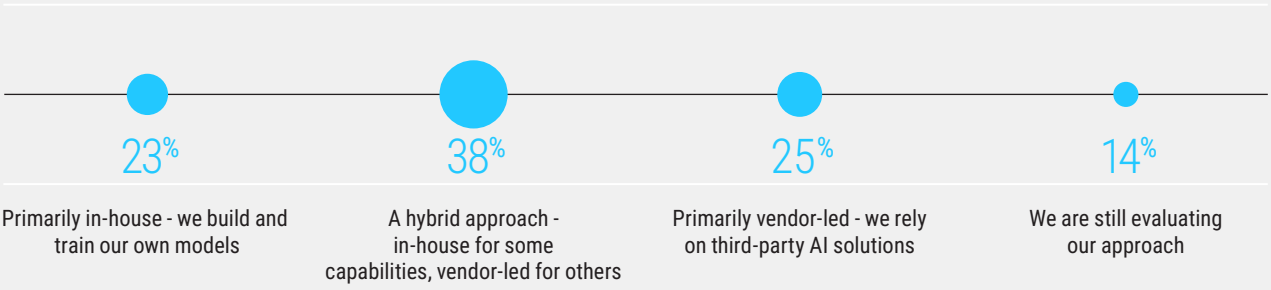
> *Applying risk-based checks at the appropriate stage of the customer journey — such as during onboarding or key transaction points — represents an important shift away from purely reactive detection. Enabling customers to validate or revalidate their identity in a low-friction way, such as through trusted devices or biometric methods like selfies, can be highly effective when applied at high-risk moments"*

Investigating AI deployment strategies and effectiveness

When it comes to how European banks are deploying AI, our survey found that organisations are preferring hybrid approaches (38%), building certain capabilities in-house while outsourcing others to specialised vendors. As the fraud landscape grows in complexity, banks are preferring to base their fraud strategies on multi-layered frameworks.

TOTAL RESPONSE

How does your institution primarily approach the development of AI capabilities for fraud prevention?



When it comes to vendor vs. in-house, the split is minimal: a quarter of banks rely primarily on third-party AI solutions, while 23% of banks primarily build and train their own models. Finally, 14% of banks are still evaluating their approach.

Yet while tools are widely adopted, our survey finds that by themselves they are rarely highly effective — highlighting that a comprehensive set of tools is needed to fight modern fraud.

TOTAL RESPONSE

For the fraud prevention controls listed below, how effective are they in practice at your institution?

Ranked on a scale of 1 to 5	1 - Highly effective	2 - Effective	3 - Partially effective	4 - Not effective	5 - Not in use	Rank[1]	Score[2]
Human intervention (via fraud specialists in bank contact centres)	36%	36%	25%	2%	0%	1	1.94
Onboarding-to-payment data linkage	25%	53%	20%	2%	0%	2	1.99
Digital ID integration (e.g. BankID, eIDAS)	29%	45%	23%	3%	0%	3	2.00
Behavioural biometrics	30%	42%	26%	2%	0%	3	2.00
Authentication signals (biometric, step-up authentication, MFA)	29%	45%	23%	3%	0%	4	2.01
Payee intelligence using consortium or shared industry data	27%	46%	25%	2%	0%	5	2.02
Network analytics and link analysis	27%	47%	23%	3%	0%	5	2.02
Device intelligence	25%	50%	21%	3%	0%	6	2.03
Real-time money mule account detection	26%	45%	28%	1%	0%	7	2.04
Confirmation of Payee (CoP) or equivalent payee verification	26%	47%	24%	4%	0%	8	2.06
Payee intelligence using own proprietary data only	20%	53%	23%	3%	0%	9	2.12

[1] based on weighted average order. [2] weighted average score to 2dp

0% 60%

Human intervention (via fraud specialists in bank contact centres) remain the most effective fraud prevention control in a bank, showcasing the importance of keeping a human-in the-loop. As fraudsters are focusing on human vulnerabilities, human-to-human conversation between customers and fraud specialists in bank contact centres remains the key tool in preventing fraud. New controls such as 'on-the phone-indicators' highlight signs of manipulation to the contact centre specialist to help guide the conversations around transactions which may have been authorised.

Human intervention (via fraud specialists in bank contact centres) is most effective in CEE, with 43% of respondents rating it as 'highly effective', 7 percentage points above the European average.

Ainsley details:

> *"Human intervention remains highly effective to protect customers, and our 'Break the Spell' team is a strong example of this. A team that helps customers understand that they've been scammed. In extreme cases, where customers have been heavily socially engineered by fraudsters, the team can spend months helping a customer realise that the person they have been speaking to and trust, is in fact a criminal trying to scam them. The team primarily speaks with customers over the phone, but also face-to-face in branch if needed. Santander's 'Break The Spell' team prevented customers from handing over £6.8 million to scammers last year [2025], bringing the total amount saved to £24.4 million since launching in 2021."*

In terms of effectiveness, 'human intervention (via fraud specialists in bank contact centres)' is closely followed by creating data linkages between onboarding and payments, while digital ID and behavioural metrics share the third place rank — all of which are effective tools for detecting unauthorised payment attempts, cases of account takeover, or money mules.

Yet notably, fraud tooling cannot be effective in isolation. In 2026 and beyond, banks can only successfully fright fraud by creating holistic data pictures and leveraging an encompassing set of fraud controls that can cover a complex range of typologies.

Top regional fraud prevention controls

DACH
Human intervention (via fraud specialists in bank contact centres) (33% 'highly effective')

Benelux
Digital ID integration & Confirmation of Payee (CoP) or equivalent payee verification (44% 'highly effective')

UK
Device intelligence (57% 'highly effective')

Nordics
Real-time money mule account detection (37% 'highly effective')

CEE
Authentication signals (47% 'highly effective')

Southern Europe
Human intervention (via fraud specialists in bank contact centres) (40% 'highly effective')

When it comes to fraud typologies, money mule activity is a consistent concern for organisations,

as it can be significantly harder to spot fraud involving accounts owned by real people (or legitimate appearing synthetic identities), involving transactions that make the illicit funds look like legitimate, everyday banking activities.

Ainsley comments:

> *Money mules are essential to most forms of payment fraud, yet the capability to detect them is often not clearly defined or fully developed. Detection frequently occurs after suspicious transactions have already taken place, rather than before or during the activity. Mule accounts can initially appear legitimate, particularly when they involve synthetic identities or have been recruited to closely mimic normal customer behaviour. In some cases, the behaviour may genuinely appear typical."*

Our survey finds that money mule detection is indeed one of the key investment areas for organisations (more about investment in chapter 6), so how would banks currently describe the operational status of their detection capabilities for money mule signals?

The survey data shows that real-time mule detection remains only semi-mature across Europe, with the majority of banks either still relying on batch-based or retrospective detection, or only deploying partial real-time capabilities.

TOTAL RESPONSE

How would you describe the current operational status of your detection capabilities for the following money mule data signals?

Ranked on a scale of 1 to 5	1 - Real-time mule detection is fully operational	2 - Partial, we detect mules but not consistently in real time	3 - Our mule detection is retrospective or batch-based	4 - Mule detection is a gap we are actively looking to address	5 - No current plans/ Not monitored
Linkage between on boarding data and payment activity	16%	34%	37%	12%	1%
Network connections to known mule or fraud accounts	18%	36%	25%	19%	2%
Outbound transaction and funds-out behaviour	17%	35%	32%	12%	4%
Changes in account credentials (address, phone number, email)	16%	36%	29%	16%	2%
Changes in account behaviour patterns	13%	39%	31%	14%	3%
Inbound transaction patterns	13%	36%	34%	12%	4%

0% 40%

05 How are European banks fighting fraud in 2026?

Linkage between onboarding data and payment activity is the most mature money mule detection tool as European banks strive to unify their data to create more holistic customer profiles. Analysing inbound transaction patterns to identify money mules sits on the other end of the spectrum, being the analysis tool that is still most reactive for banks.

Dave Laramy, ex-head of fraud at Danske Bank, now global head of fraud at Klarna expands:

> *"The key challenge with tackling money mules is time. Money moves instantly and investigating what has happened when not everyone is telling the truth takes time. Banks must collect the evidence available and make decisions on the balance of probabilities. Appropriate data sharing across banks provides more of the facts and is absolutely needed in real-time to tackle the problem together."*

UK banks are the most mature across Europe for linkage between onboarding data and payment activity, with one in three already in real-time mule detection, 17 percentage points above the European average.

Ainsley adds:

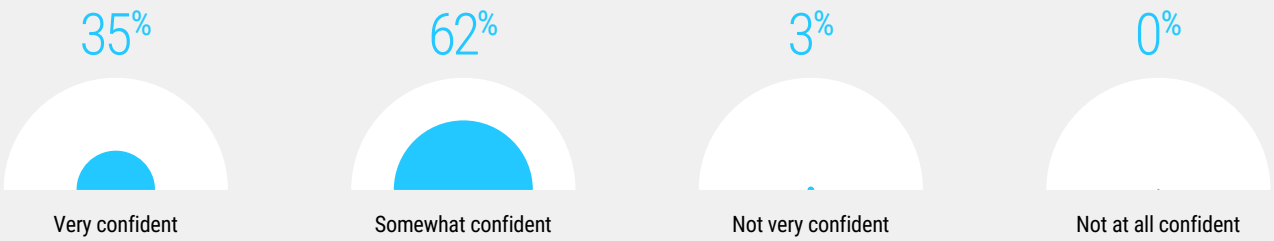
> *"Effective real-time decisioning requires low-latency data integration across multiple systems, as well as well-trained models specifically designed to detect mule activity — something that is often difficult to achieve. Organisational silos between fraud, AML, and payments teams further slow down the development of unified responses. To address these challenges, firms should invest in consortium data, real-time capabilities, and post-event analytics. They should also adopt network-based detection approaches to identify mule activity and linked accounts more effectively. However, this is not a silver bullet. Firms should combine payments data with behavioural signals and onboarding risk indicators to build a more holistic view of customer activity, while also developing proactive methods to detect earlier signals of fraud."*

06 What's next? Investigating fraud investment plans and barriers

Considering the speed at which fraud typologies are evolving, combined with the fact that current fraud detection tools are rarely fully effective, it comes as no surprise that the majority of European banks (62%) are only 'somewhat confident' that their current capabilities are adequate to address the fraud threats over the next three years.

TOTAL RESPONSE

How confident are you that your current fraud prevention capabilities are adequate to address the threat environment over the next three years?



While nearly all banks across the region are at least somewhat confident (97%), only just above one in three (35%) are very confident in their capabilities in the near future, indicating that most banks believe that while they are poised to handle growing fraud numbers, the evolving fraud landscapes requires more advanced tools and controls.

Only 20% of Nordic banks are 'very confident' in their fraud prevention capabilities over the next three years, ranking 15 percentage points below the European average. Another 13% are 'not very confident', showcasing the regions' concern about evolving threat levels.

There are many factors that affect an organisations confidence in their fraud prevention strategies. So, what are the key roadblocks? The responses show that data quality or data access limitations are the key barriers to improving fraud prevention capabilities, followed by organisational silos as well as a lack of skilled fraud technology talent.

TOTAL RESPONSE

What is the single biggest barrier to improving your institution's fraud prevention capabilities?

Data quality and access limitations perhaps unsurprisingly remain the key challenge in effective fraud prevention, because while internal data is one side of the coin, truly effective fraud strategies necessitate wider ecosystem data and industry collaboration.

Martin emphasises:

> *"The organisations that are proving most resilient are those investing in risk led, data driven approaches and deep collaboration, both within their own ecosystems and across the wider industry. They're recognising that fraud is now a shared, system level problem rather than a purely local one. We need cross sector and cross industry collaboration to fight this growing threat."*

Stervinou explains that both in France and in the EU, these initiatives are increasingly looked at. In light of rising fraud numbers, the Banque de France has helped establish:

> *A national platform of suspicious IBANs, which since May this year enables French PSPs to share fraud-related data in compliance with the GDPR, following the adoption of a specific French law against banking fraud. Such data-sharing mechanisms are expected to be extended at the EU level under the forthcoming Payment Services Regulation (PSR).*"

However, while data is a key concern across all regions, the picture becomes more fractured as we look more deeply at the different European markets.

Top regional barriers to improving fraud capabilities

DACH
Organisational silos between fraud, technology and compliance functions (24%)

Benelux
Organisational silos between fraud, technology and compliance functions (22%)

UK
Lack of skilled fraud technology talent &
Data quality or data access limitations (both 23%)

Nordics
Data quality or data access limitations (27%)

CEE
Regulatory uncertainty (23%)

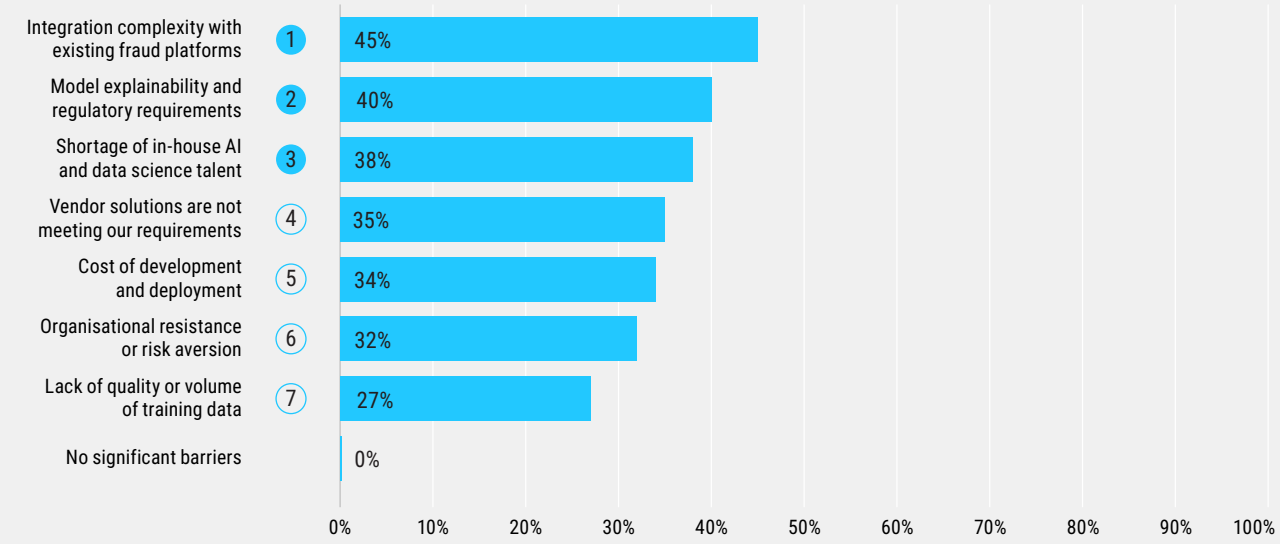
Southern Europe
Vendor or solution limitations (23%)

When it comes to the technology itself, the biggest challenge in expanding AI adoption across fraud strategies and tools continues to be the complexity of the integration of AI with existing fraud platforms.

TOTAL RESPONSE

What are the greatest barriers to expanding AI adoption in fraud prevention at your institution?

Select up to three options



Model explainability and regulatory requirements play another crucial role in AI expansion, which comes as no surprise considering the EU was the first region globally to roll out comprehensive AI compliance requirements with the EU AI Act.

The lack of quality or volume of training data ranks last, remaining a challenge for roughly 1 in 4 banks (27%). It's not only the growing number of fraud itself that provides training data for banks, but the availability of generative AI and its capabilities to generate synthetic data have equally helped banks improve their access to relevant training data for the improvement of fraud models.

Ainsley comments:

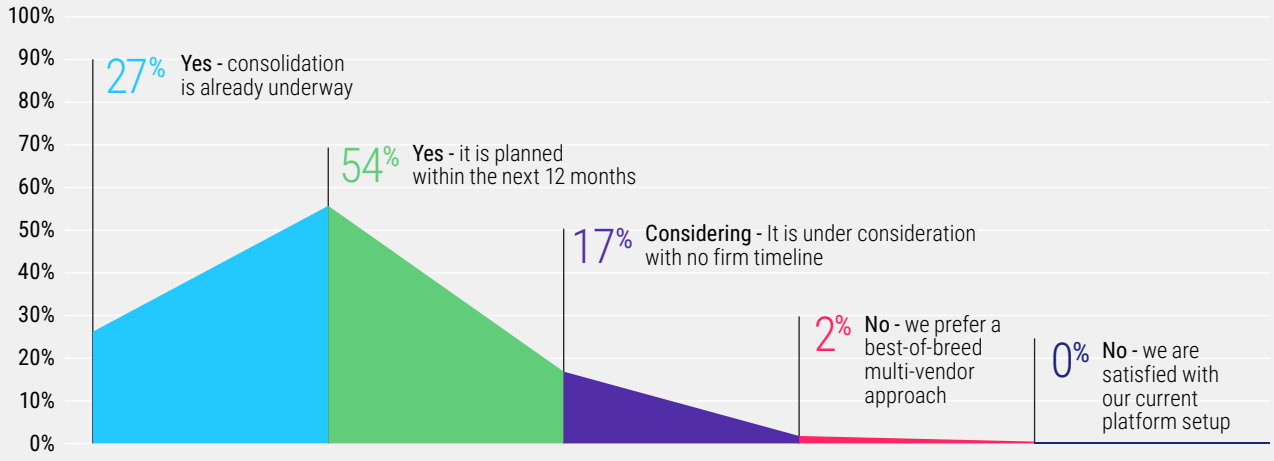
> *"There are several challenges in orchestrating modern fraud controls. Many organisations operate with fragmented control stacks involving multiple vendors and inconsistent data signals. There is also a trade-off between latency and accuracy in real-time decisioning. Banks must carefully manage the balance between customer experience and the introduction of friction to prevent fraud. The absence of a single, unified decisioning layer further complicates orchestration, particularly as fraudsters continuously adapt their tactics."*

Planning ahead — examining the key investment priorities for European banks

Considering fragmentation remains a challenge, and to Ainsley's point, our survey data finds that four out of five European banks are actively planning or already executing the consolidation of multiple fraud risk engines into a unified platform.

TOTAL RESPONSE

Is your institution actively looking to consolidate multiple fraud risk engines or vendors into a single unified platform?



While 27% of banks are already in the process of consolidating, the majority (54%) are planning their consolidation over the next 12 months — highlighting that complexity is a key concern that organisations are trying to address in order to reduce operational complexity and improve detection efficiency.

Laramy speaks on the impact of platform consolidation:

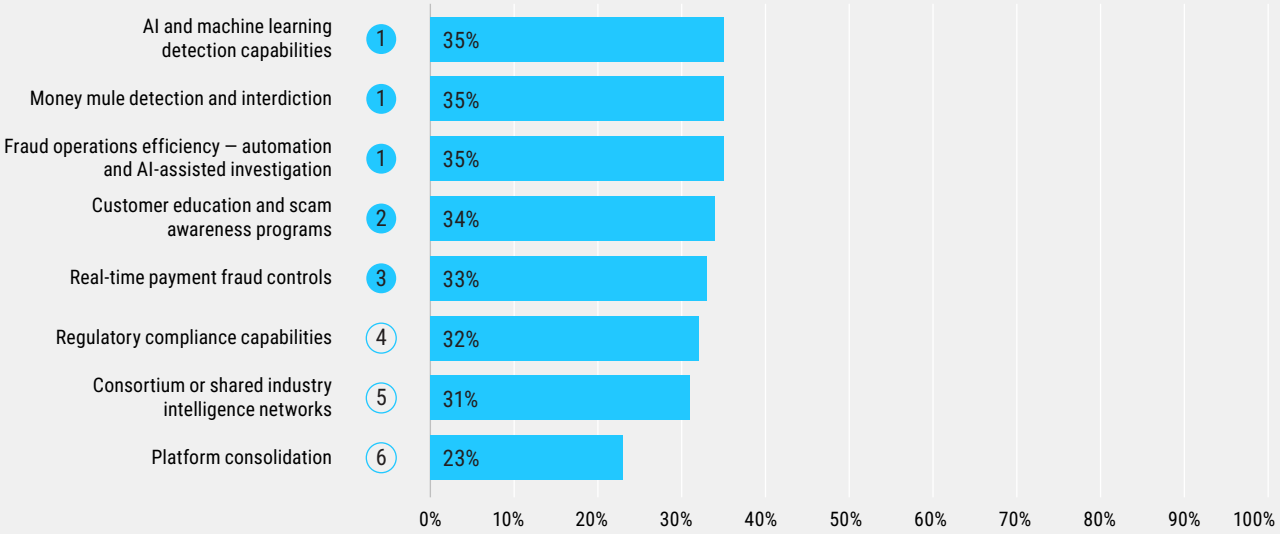
> *Having all the data in one place provides greater coverage and agility to manage fraud throughout the customer lifecycle. Rules can be built with more data attributes and models can be built quickly using expanded data now readily available on the platform. Contingency options such as alternative strategies ready to go, error handling options and technical incident management all become more important when you have a single platform."*

In terms of investment, while platform consolidation is a key strategic initiative for most banks, they are at the same time not investing a large chunk of their budgets into the process itself. Even though consolidation is cited as crucial for the majority of banks, the urgent investment areas lie elsewhere.

TOTAL RESPONSE

What are your institution's primary areas of planned investment in fraud prevention over the next 12-24 months?

Select up to three options



The key priorities in terms of investment over the next one to two years lie in AI and machine learning detection capabilities, money mule detection and interdiction, as well as fraud operation efficiency — all of which are a priority for 35% of European banks.

However, looking at the investment plans more granulary, AI and machine learning capabilities are high on the list for all European markets, yet regional priorities emerge that are worth highlighting.

Top regional investment priorities

DACH
AI and machine learning detection capabilities (52%)

Benelux
Fraud operations efficiency (44%)

UK
Money mule detection and interdiction & Regulatory compliance capabilities (both 40%)

Nordics
Real-time payment fraud controls & Customer education and scam awareness programs (both 40%)

CEE
Real-time payment fraud controls (53%)

Southern Europe
Customer education and scam awareness programs (50%)

As each European region grapples with its own markets' idiosyncrasies, the overall trend is clear: in order to fight AI-enabled, industrialised fraud, detection and prevention strategies are needed that similarly leverage AI and target not only the complex, real-time nature of fraud, but also human vulnerability as a key fraud vector.

Crucially, the adjustment of regulatory frameworks is additionally designed to help European banks tackle an increasingly complex fraud environment.

Stervinou finalises:

> *Looking ahead, the forthcoming EU regulatory framework (PSD3/PSR) is expected to further strengthen the fight against fraud. We are particularly looking forward to the establishment of the future EU platform to combat fraud, that is designed to operate in a manner similar to the OSMP, as it will further enhance coordination within the European payment ecosystem and, therefore, our global efficiency."*

07 Conclusion

As several macrotrends are shaping the European fraud landscape — the expansion of instant payments, shifting regulatory expectations, and the industrialisation of fraud itself through AI — banks are racing against the clock to fortify controls and strategies.

So, what does an effective fraud framework look like?

Ainsley concludes:

> *An effective approach involves a central decisioning engine capable of orchestrating identity signals, device intelligence, transaction context, and behavioural analytics. This enables consistent risk scoring across all channels in real time, creating a more cohesive fraud prevention framework. However, this also requires flexibility in how outcomes are deployed across channels, such as updating warnings or introducing dynamic customer interactions — capabilities that many existing architectures were not designed to support."*

In 2026 and beyond, the banks that will be the most effective at this will be the ones that move away from point-in-time controls and detection-led approaches towards real-time authentication and monitoring as fraud prevention has moved away from being a balance sheet exercise into being a competitive differentiator.

08 About

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers. The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information:
Visit **www.finextra.com** and become a member,
follow **@finextra** or reach us via **contact@finextra.com**.

NICE Actimize

As a global leader in artificial intelligence, platform services, and cloud solutions, NICE Actimize excels in preventing fraud, detecting financial crime, and supporting regulatory compliance. Over 1,000 organisations across more than 70 countries trust NICE Actimize to protect their institutions and safeguard assets throughout the entire customer lifecycle. With NICE Actimize, customers gain deeper insights and mitigate risks.

Learn more at **www.niceactimize.com**.

Finextra

Finextra Research Ltd
77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

+44 (0)20 3100 3670

contact@finextra.com

www.finextra.com