Global Insights 2025

Predictions from Experian

The key themes and emerging trends shaping financial services in 2025, using research and **insight from leading industry analysts**

1. Fraud evolution driven by AI
2. AI will play a transformative role in banking
3. Emergence of RegTech
4. Convergence of risk management

experian.

Contents

Fraud evolution driven by AI

In response to the alarming increase in fraud incidents fuelled by the increasing use of AI, fraud prevention continues to be a top investment priority for banks in 2025.

Two-thirds of businesses believe they are denying good customers over fear of fraud

Redefining risk management: Driving growth in financial services through credit, fraud, and compliance convergence, Experian 2024

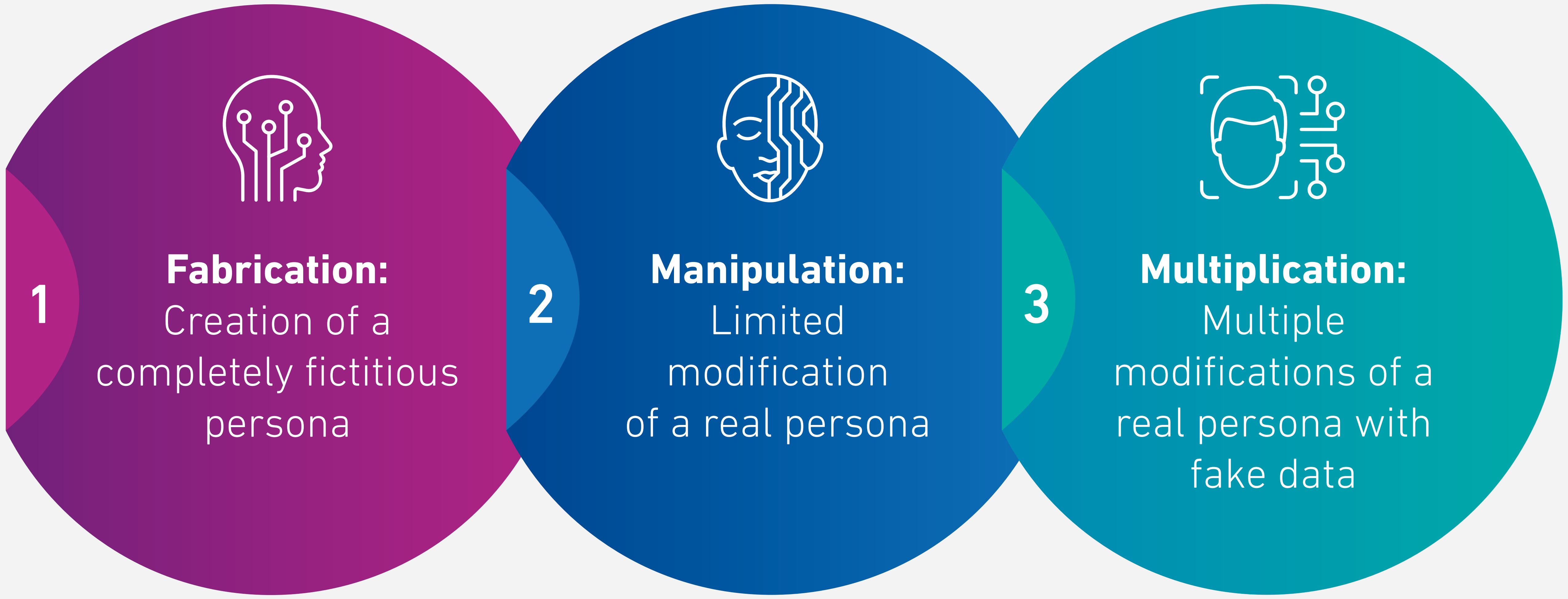
Threats from GenAI*-fuelled synthetic identity fraud

Challenges associated with tracking synthetic identity fraud make it one of the biggest concerns for 2025

Synthetic loan applications will grow **100%** by 2027, resulting from the availability of GenAI and personal data on the dark web.[1]

Synthetic identity: A combination of real and fake identity data engineered to appear as an authentic identity

Criminals typically combine real and fake data in three main ways:



1 **Fabrication:** Creation of a completely fictitious persona

2 **Manipulation:** Limited modification of a real persona

3 **Multiplication:** Multiple modifications of a real persona with fake data

By stealing data and using advanced technologies, fraudsters can create an identity that appears as authentic

* *GenAI: AI techniques that learn a representation of artefacts from data and use it to generate brand-new, unique artefacts*

[1] *IDC FutureScape: Worldwide Retail Banking 2025 Predictions, doc #US52634924, October 2024*

Building a synthetic identity

Criminals now use stolen information to create highly realistic synthetic identities supported by AI-generated videos, fabricated backstories, forged documents and employment records, fake social media profiles, and other evidence to legitimise their scams. This makes it nearly impossible for traditional fraud detection systems to distinguish real from fake applicants

Fraudsters are using GenAI to create deepfakes, fake IDs, and manipulate live video and audio, revealing how such attacks can deceive both individuals and enterprise systems

Voice-cloning scams, another GenAI-driven threat (where voices can be replicated with up to 85% accuracy from as little as three seconds of audio), have already caused individual losses ranging from $500 to $15,000, with financial institutions facing broader implications for failing to catch such scams

Lack of standardised definitions:

The absence of consistent definitions and classification frameworks hinders accurate tracking and mitigation of synthetic identity fraud. This inconsistency makes it difficult to measure synthetic fraud's prevalence and associated mitigation strategies.

Misclassification: Some institutions might classify fraud involving authentic and synthetic data as identity theft, while others classify it as synthetic fraud

Misclassification and unsorted data:

Synthetic identity fraud is often confused with other types of fraud, like first-party fraud or miscategorised as credit losses. These fraud losses frequently overlap with credit loss categorisations, especially during defaults, further complicating tracking and mitigation efforts.

Complexity of detection:

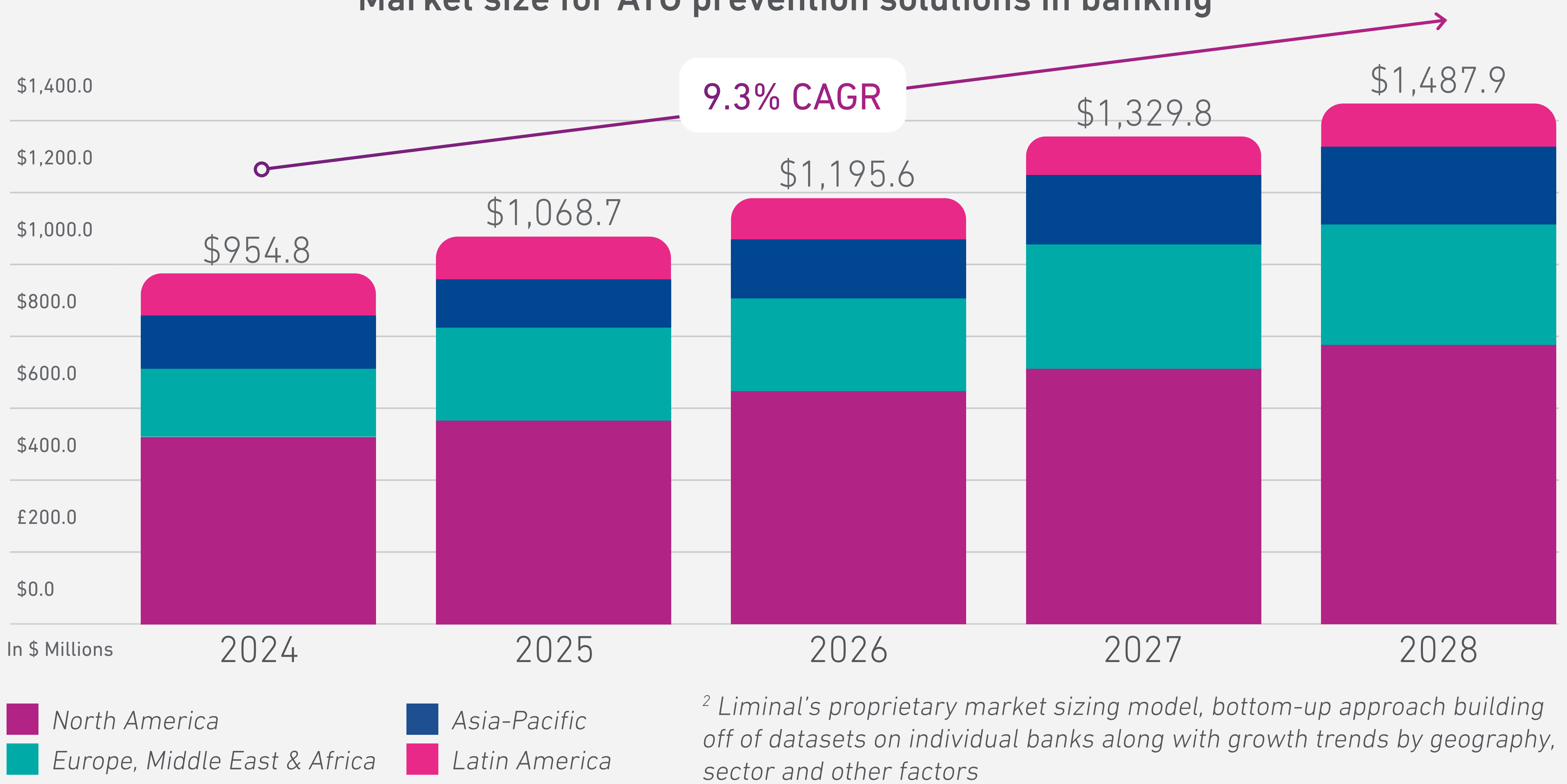
Traditional fraud detection systems struggle to identify sophisticated synthetic identities. Detecting fraud generated by AI, like synthetic identities, upstream in the fraud creation process is difficult.

Industry experts emphasise the need for banks to invest in advanced AI-powered tools within a layered approach to combat synthetic identity fraud at verification. This includes solutions that leverage machine learning, behavioural analytics, device intelligence, and consortium-based data sharing to identify and mitigate synthetic identities.

Account takeover (ATO) fraud, when criminals gain access to existing accounts using stolen credentials, remains a significant concern for 2025. This trend is exacerbated by the vulnerability of traditional authentication methods, from phone one-time-passwords (OTP), to social engineering (now fuelled by accessible GenAI tools) and interception tactics, such as man-in-the-middle attacks, where an undetected attacker intercepts or manipulates communication between two parties.

Defending against ATO requires prioritised investments in multi-factor authentication and real-time fraud detection systems that can identify suspicious login attempts and account activity. This includes leveraging machine learning, behavioural biometrics, and device intelligence to analyse customer interaction patterns and detect anomalies that could indicate an account takeover.

Market size for ATO prevention solutions in banking[2]



[2] *Liminal's proprietary market sizing model, bottom-up approach building off of datasets on individual banks along with growth trends by geography, sector and other factors*

The global TAM for ATO prevention in banking is projected to grow from **~$954.8 million** in 2024 to **$1.5 billion** by 2028, with a compound annual growth rate **(CAGR) of 9.3%**

Liminal's Link Index for ATO Prevention in Banking Report

APP scams and social engineering:

2025 is likely to see a continued surge in APP scams, where victims are tricked into authorising payments to fraudsters, often facilitated by money mules[3]. The increasing sophistication of social engineering tactics used to manipulate victims makes these scams particularly challenging to combat. In the EU and UK, liability shifts place greater responsibility on banks, making robust identity verification of payees and payers critical

[3] *A type of money laundering: Someone who lets criminals use their bank account to move money.*

Adaptability, proactive strategies and collaboration

Fraudsters are constantly evolving their tactics, especially by leveraging AI. Banks need to partner with vendors who offer advanced analytics, real-time fraud detection, and tools to simulate and counter future threats.

Collaboration is more crucial than ever. Experts emphasise the importance of interbank data sharing, and consortium-based approaches to combat sophisticated fraud, enhance detection capabilities, and gain broader insights into emerging trends.

Authorised Push Payment (APP) fraud is expected to grow at 11% CAGR from 2023 to 2027

McKinsey, Global payments in 2024: Simpler interfaces, complex reality

AI will continue to fuel more sophisticated attacks across the consumer lifecycle, enabling fraudsters to attack at scale. This includes:

- GenAI-driven synthetic identity creation, paired to seemingly authentic "proof of life" indications like fake social media accounts, and AI-generated identity images.
- AI will help fraudsters craft highly personalised and more credible phishing attacks and phishing sites for capturing stolen credentials, which fraudsters will use to take over legitimate accounts. This may include family-member or business-associate impersonation ploys, where fraudsters use images, audio and videos from social media to replicate highly personalised scams.
- Creating automated attacks at scale with an ability to distribute attacks across the full lifecycle.

> This year, we expect to see the most sophisticated threats emerge as AI continues to fuel attacks across the entire consumer lifecycle. This will drive the need for businesses to apply AI against a wider set of signals to distinguish between good and bad actors. Layering together behavioural signals, device intelligence, authenticated identity and biometrics data, plus powerful consortium data, will help to fight these threats. Layering AI on top of signals allows businesses to distinguish good from bad actors instantly, highlight the top risk factors, find similar cases, and even suggest next steps. This allows teams to spend less time parsing data, and more time blocking attacks – helping everyone stay a step ahead of evolving fraud tactics.

David Britton,
VP of Strategy,
Global Identity and Fraud,
Experian

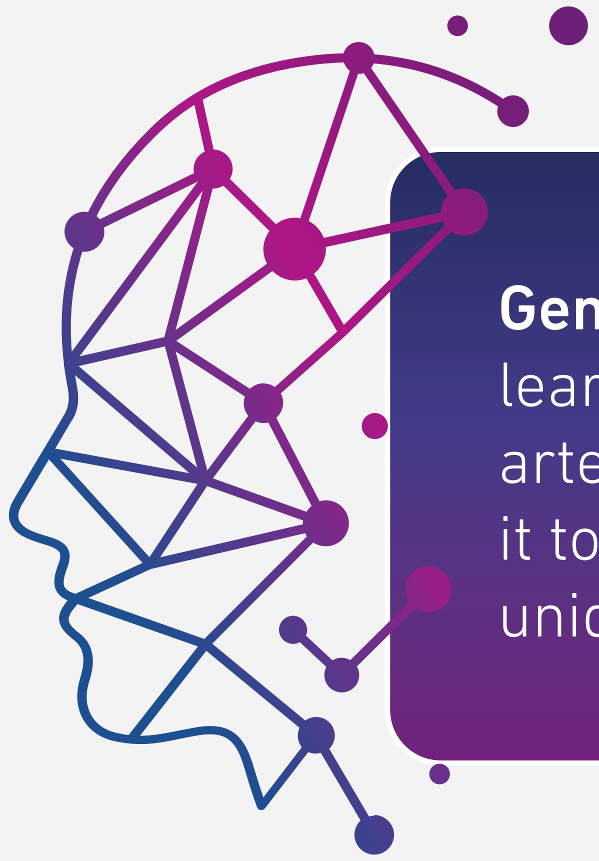
AI will play a transformative role in banking

A surge in the development and adoption of GenAI tools is expected in 2025 and beyond. Global spending on AI has significantly increased, with GenAI experiencing particularly rapid growth. This financial impetus fuels ongoing research, development, and deployment of new AI-powered tools and solutions.

The rapid growth in GenAI investments will enable the category to outpace the overall AI market with a five-year CAGR of 59.2%.

By 2028, IDC expects GenAI spending to reach $202 billion, representing 32% of overall AI spending

From GenAI to Agentic AI



GenAI: AI techniques that learn a representation of artefacts from data and use it to generate brand-new, unique artefacts

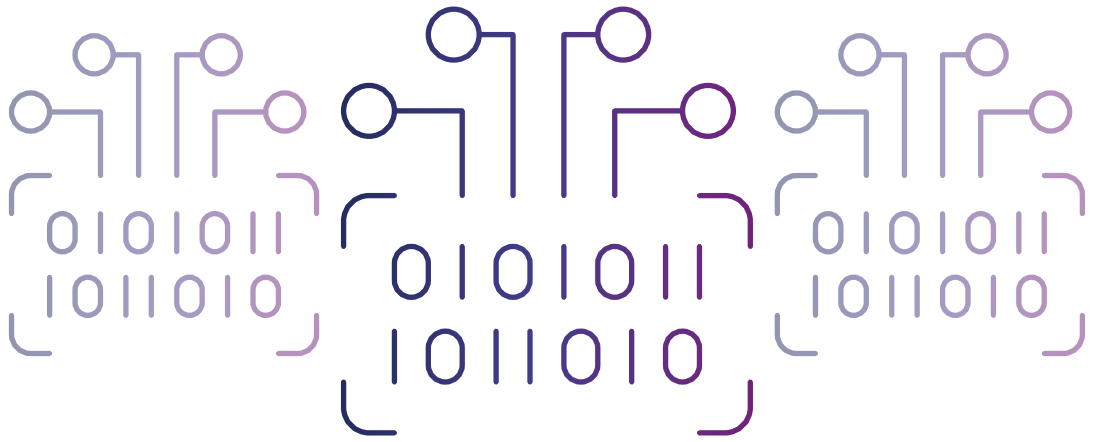
Agentic AI: AI systems that autonomously solve complex, multi-step problems using sophisticated reasoning and planning. These systems can perceive data, reason through tasks, take actions, and learn from feedback

The proliferation of GenAI has created a demand for automation, efficiency, and hyper-personalised customer experience (CX). However, experts observe greater caution in GenAI adoption by financial institutions due to the critical nature of decisions and regulatory requirements. Businesses prefer using GenAI for data preparation and model suggestion rather than allowing it to make autonomous decisions.

Data science-centric GenAI, trained on analytics and data science workflows, focuses on data cleaning, transformations, data joining, code generation, and model diagnostic reports for compliance documentation and makes ideal ‘assistants’ in model development. These tools free up valuable full-time equivalent (FTE) time for other strategic initiatives.

Assistant: Users interact live with a virtual assistant, offering bespoke guidance and code generation for software, powered by GenAI.

As GenAI use cases begin to prove value, Agentic AI is capturing the attention of businesses. Organisations are starting to explore AI agents that go beyond GenAI and have an action component.



Agentic AI example:
Microsoft has introduced agentic capabilities into Copilot to allow every organisation to have a constellation of agents to execute and orchestrate business processes.

As further advancements in AI develop and open up opportunities, companies are still facing challenges.

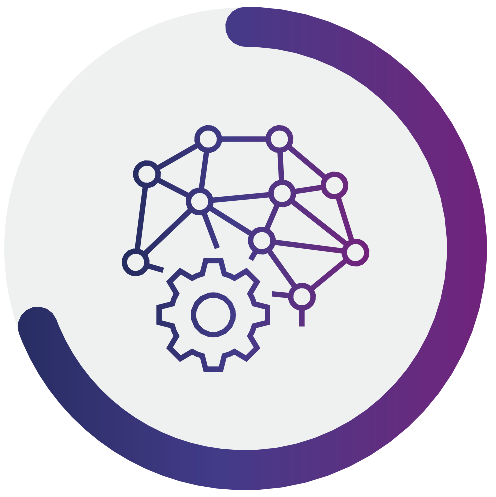
Responsible AI is no longer optional

The potential of AI and GenAI to revolutionise financial services has been researched and written about more in 2024 than ever before. However, even with all this potential, there are also challenges.

Banks should anticipate regulatory drivers for adopting Responsible AI (RAI), the most prominent being those focused on ensuring fair and ethical applications. According to IDC[4], by 2027, 70% of tier one global banks will have set up a dedicated compliance function with a holistic approach in response to the ever-stringent responsible AI regulations. These aim to establish clear guidelines and requirements for AI development and deployment. This drives the need for financial institutions to adopt RAI frameworks to ensure compliance.

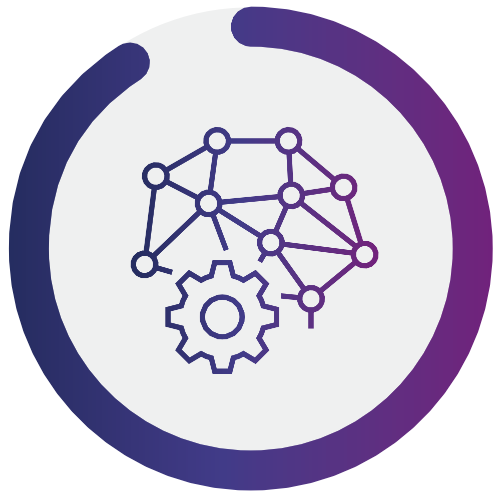
[4] *IDC FutureScape: Worldwide Retail Banking 2025 Predictions, doc #US52634924, October 2024*

In a survey conducted by McKinsey among 100 companies with annual revenues >$50m:



63%

of respondents categorised the implementation of GenAI as a "very high/ high" priority for their organisation



91%

thought that they were "not prepared" to do it responsibly

Three out of four firms that build aspirational agentic architectures on their own will fail.
AI agentic architectures were a top emerging technology for 2024, but they're not ready yet — expect another two years before they have any chance of meeting inflated automation hopes.

"Predictions 2025: Artificial Intelligence", Forrester Research

Organisations will need explainable and transparent processes

Challenges associated with GenAI could influence the pace and direction of tool development in 2025. The need for explainability in AI-driven decisions remains a significant challenge. Developers of GenAI tools will need to prioritise building transparency into their solutions, allowing users to understand how AI-generated results are derived while ensuring compliance with regulatory requirements.

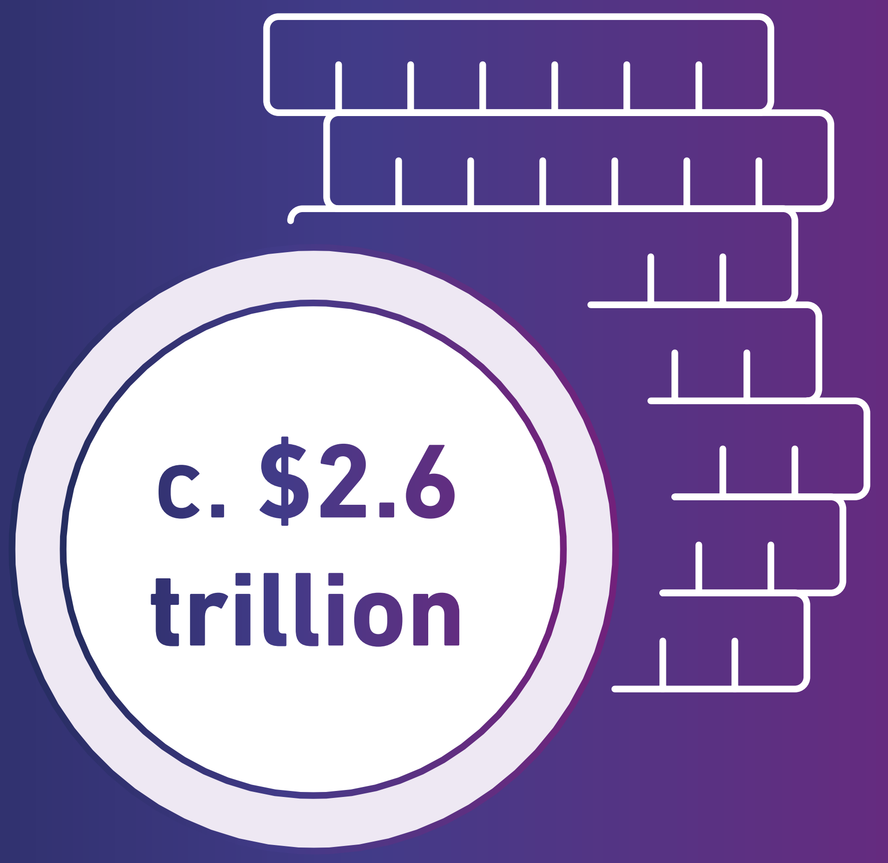
Financial institutions are hesitant to fully trust GenAI for decisions in sensitive domains like credit risk, fearing bias, errors, or lack of explainability. The demand for AI is to support decision-making, not replace it outright.

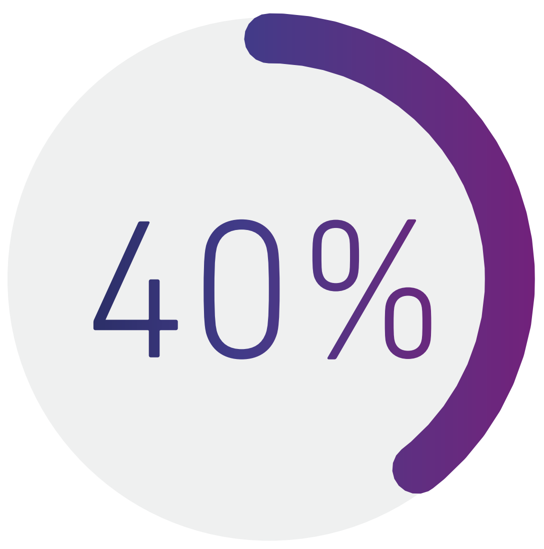
Many decisioning platforms are ready to absorb GenAI models and run them efficiently. However, businesses may resist adoption due to concerns over transparency, governance, and accountability.

Despite these challenges, GenAI tools will play a larger role in banks' strategies and proliferate in the market by 2025. This momentum is reinforced by the anticipated ramp-up in GenAI applications across industries, driven by technological advancements and the growing demand for AI-powered solutions to address evolving business needs.

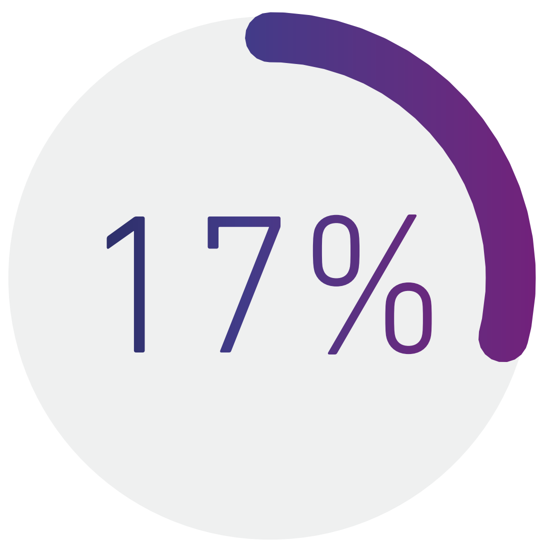
McKinsey estimates that the banking sector could account for $200bn-$340bn of the estimated $2.6 trillion in annual value that GenAI is expected to add globally, with the impact being felt across virtually every business function.

McKinsey estimates the annual global added value from GenAI will be:

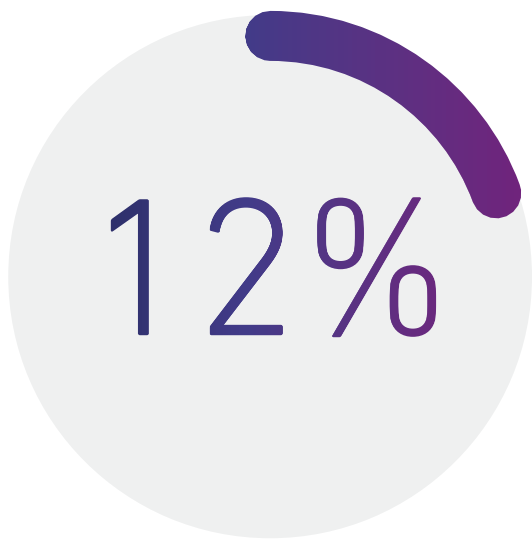




of organisations identify explainability as a key risk in adopting GenAI

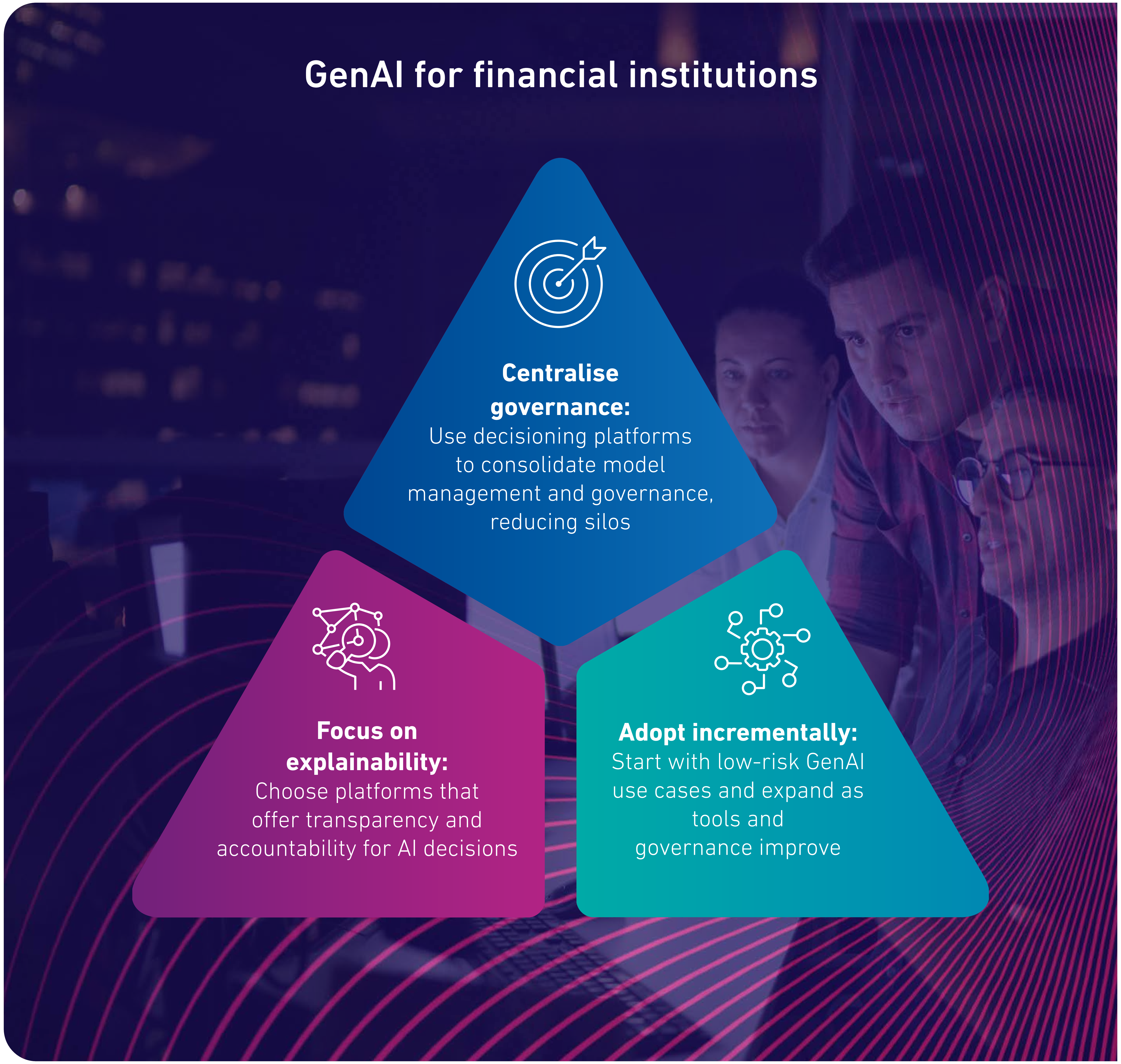


of organisations are trying to mitigate the risk of GenAI explainability



of the organisations that have adopted GenAI have experienced negative consequences related to GenAI explainability

McKinsey Global Survey on AI



GenAI for financial institutions

Centralise governance: Use decisioning platforms to consolidate model management and governance, reducing silos

Focus on explainability: Choose platforms that offer transparency and accountability for AI decisions

Adopt incrementally: Start with low-risk GenAI use cases and expand as tools and governance improve

> Generative AI is poised to revolutionise how banks tackle analytics in 2025, but there's no one-size-fits-all playbook. The best way forward is incremental: start with low-risk use cases and give data scientists real control over the code, so everything remains transparent and fully auditable. With guardrails like clear model documentation and feedback loops, financial institutions can cut development time without sacrificing regulatory confidence or model accuracy.

Keith Weitz,
SVP, Head of Global Analytics,
Experian

Emergence of RegTech to meet complexities of compliance

The global compliance environment is poised for significant transformation in 2025. Financial institutions will face heightened regulatory scrutiny, driven by evolving technology and the increasing sophistication of fraud schemes. Businesses will need to adopt innovative compliance strategies and technologies to stay ahead of regulatory demands and protect against emerging threats.

87%

of organisations are looking to introduce more automation

Experian Research, 511 senior leaders surveyed in financial services, August 2024

Regulatory pressures will only intensify, placing more scrutiny on banks

More stringent guidelines from regulatory agencies worldwide will require financial service providers to establish robust risk management practices and adopt technology that matches the scale and speed of compliance requirements.

> A wide range of regulatory frameworks including SS1/23 and SR11-07 place increasing pressures on financial institutions when it comes to compliance processes

Compliance needs that technology will support

Responsible AI (RAI) Frameworks: Compliance with regulations (EU AI Act, GDPR, U.K. FCA, U.S. Algorithmic Accountability Act, NIST) requires transparent, fair, and explainable AI. Tools that automate impact assessments, enhance documentation, and simplify conformity ensure RAI compliance and operational efficiency in high-stakes areas like fraud and credit risk.

Modernising for operational resilience: Global and regional regulations (EU Digital Operational Resilience Act, Australia's Cross-industry Prudential Standards) demand modern architectures for risk management, incident reporting, and resilience testing. Integrated solutions for automated reporting and coordinated testing help banks stay compliant and maintain service continuity.

Driving data governance and explainability: Privacy laws and risk management regulations require data minimisation, purpose limitation, security, and clear AI model documentation. Solutions must offer flexible storage, real-time monitoring, and automated reporting to ensure transparency, impartiality, and compliance.

> As the global compliance landscape undergoes significant transformation in the upcoming years, leading financial institutions are proactively adopting innovative RegTech solutions. These solutions are set to address increased regulatory scrutiny alongside the need to maintain consistency across all models and frameworks within the institution. Prioritising the integration of responsible AI frameworks, modernising for operational resilience, and enhancing data governance will be essential for maintaining compliance and ensuring operational efficiency.

Ankit Sinha,
Senior Director of Product
Platforms and Software, FSD
(Financial Services and Data)
Experian

Convergence of risk management

Convergence isn't just a trend – industry experts believe it has the potential to reshape the industry, and financial institutions are starting to recognise this.

say forward-looking companies will centralise fraud, credit risk and compliance functions

Redefining risk management: Driving growth in financial services through credit, fraud, and compliance convergence, Experian 2024

The convergence trend: Banks are starting to navigate fraud mitigation, compliance management, and credit risk simultaneously

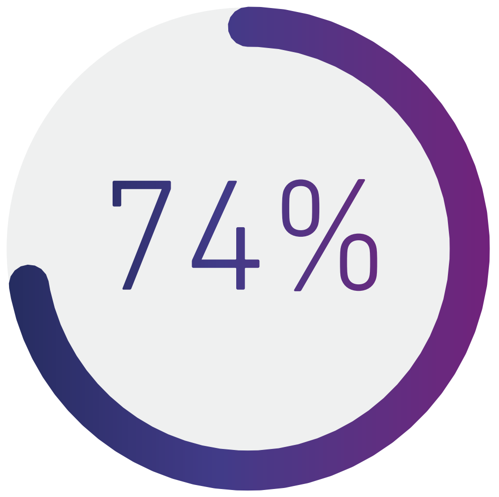
Integrating digital identity

As financial institutions unify their fraud, credit risk, and compliance efforts, digital identity emerges as the linchpin that ties these converged functions together.

Identity verification is central to fraud prevention, ensuring individuals are who they claim to be. Reducing friction for consumers to achieve portfolio growth is a key aspect of the convergence trend, and a robust digital identity framework is essential for its success.

Fraudsters are adopting increasingly sophisticated methods that capitalise on advancements in GenAI and the availability of personal data, posing unprecedented challenges to financial institutions.

Juniper predicts global digital identification spending will grow by:



from $15.2bn in 2024 to $26bn in 2029, driven by innovations like behavioural biometrics which streamline verification and improve fraud detection efficiency

By 2028, Gartner predicts that 50% of enterprises will adopt advanced tools for detecting synthetic identities and improving authentication (compared to less than 5% in 2024), while AI-powered identity verification systems are becoming essential for analysing behavioural patterns, device intelligence, and geolocation data to create holistic customer risk profiles.

Defining convergence: Convergence in the credit risk, fraud risk, and compliance space refers to the blending of operations or strategy teams, shared technology across organisational functions, or joint data and the use of common analytics tooling and infrastructure.

Redefining risk management: Driving growth in financial services through credit, fraud, and compliance convergence, Experian 2024

Industry experts agree that modern machine learning techniques are enabling high-performance models that process vast datasets in real-time, enhancing both fraud detection and predictive outcomes

A 2024 study found that nearly

50%

of internet traffic in 2023 was bot-generated, with many bots mimicking legitimate behaviours for malicious purposes

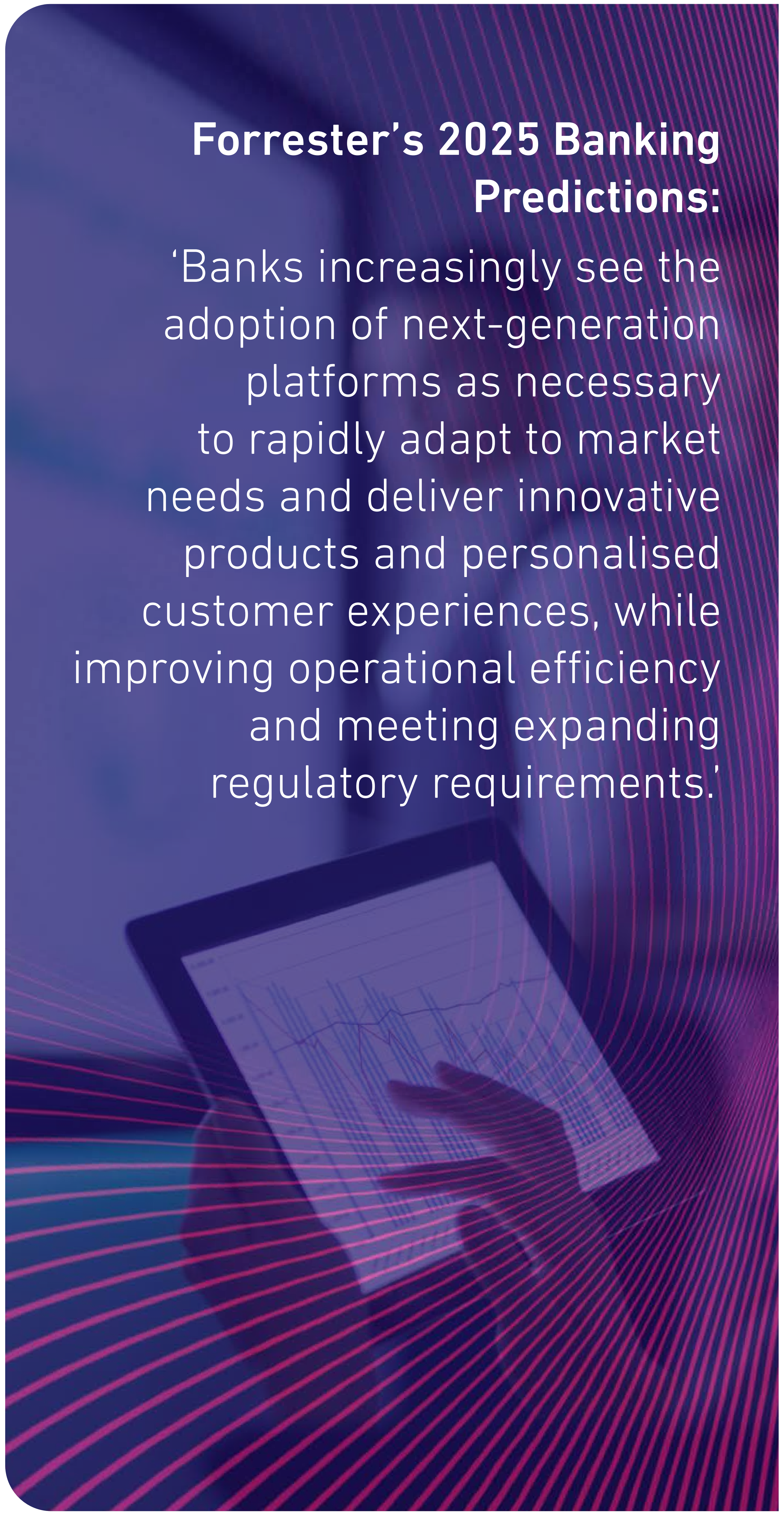
By anchoring converged strategies in a well-defined digital identity, institutions can more effectively combat emerging threats such as synthetic identities and bot-driven attacks, while simultaneously unlocking the agility and scale required to adapt to evolving market conditions.

Convergence for fraud and credit risk: Integrating insights from credit and fraud processes means institutions can detect synthetic and traditional identity fraud and digital attacks including bot activity more easily. This synergy leads to more accurate credit risk assessments and robust fraud prevention, creating a safer and more reliable risk strategy.

Breaking down siloes in tech, data and analytics across the customer lifecycle

Banks are beginning to look beyond the isolated and complex siloed functions of credit risk, fraud risk and compliance. They are increasingly seeking solutions that are holistic, integrating data, analytics, and emerging technologies to address overlapping risks and opportunities.

The same data that helps identify fraud can also assess credit risk and support compliance efforts. This realisation is driving the adoption of unified platforms that break down data silos and enable a more comprehensive view of the customer lifecycle.



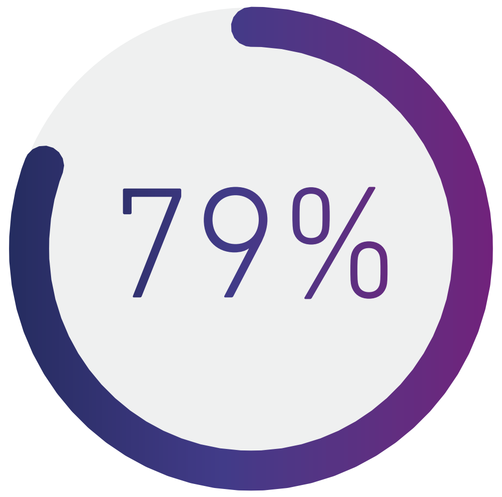
Forrester's 2025 Banking Predictions:

'Banks increasingly see the adoption of next-generation platforms as necessary to rapidly adapt to market needs and deliver innovative products and personalised customer experiences, while improving operational efficiency and meeting expanding regulatory requirements.'

Banks will drive vendor consolidation and strategic partnerships

There is a strong desire among banks to consolidate vendors and streamline vendor management practices. This is driven by:

- **Market fragmentation:** The market is saturated with vendors offering similar solutions, creating complexity and inefficiency for banks managing multiple partnerships.
- **The need for integrated solutions:** Banks are seeking holistic platforms that can address their needs across fraud, compliance, and credit risk. This requires vendors to provide integrated offerings and seamless interoperability between systems.
- **Focus on efficiency and agility:** Banks are prioritising solutions that enable them to respond more effectively to emerging threats, streamline operations, and adapt to changing market conditions.



of FI respondents say they want to work with fewer vendors to manage credit risk, fraud and compliance

Redefining risk management: Driving growth in financial services through credit, fraud, and compliance convergence, Experian 2024

> An increasing number of financial institutions are converging credit, fraud, and compliance functions to stay competitive. Streamlining processes, reducing vendor complexity, plus meeting market needs and regulatory requirements are crucial. Aligning these areas improves risk management, reduces fraud losses, and balances revenue growth with fraud prevention.

Heather Grover,
VP of Product, Ascend Platform,
Experian

December 2024

Redefining risk management: Driving growth in financial services through credit, fraud, and compliance convergence

Enhancing efficiency, insights, and growth through integration to transform the future of risk strategy

[illegible]

experian

To find out more about convergence, read our **Redefining risk management: Driving growth in financial services through credit, fraud and compliance convergence report**

Contributors:

Michael Touchton, *Senior Manager of Analyst Relations*
Rebecca McGrath, *Global Content Marketing Manager*
Matthew Stennett, *Brand Design Manager*
Enrique DeDiego, *Director of Portfolio Strategy*
Anita Nikolova, *Strategy Manager*
Paulina Yick, *Global Director of Product Marketing*
David Britton, *VP Strategy, Global Identity & Fraud*
Keith Weitz, *SVP, Head of Global Analytics*
Ankit Sinha, *Senior Director, Product Management*
Heather Grover, *VP of Product, Ascend Fraud Platform*