Mitek

Identity Intelligence Index

How banks, young and mature, can protect and delight their customers

2024

miteksystems.com

Chapters

Executive Summary

Executive Summary

A window into the identity landscape

The first edition of the Identity Intelligence Index 2024 comes at a time of anxiety for banks. They anticipate change, however their confidence in delivering the best possible customer experience is being stifled by evolving fraud risks and ever-changing regulations.

The deluge of information banks must sift through before making any change - from regulators, customer insights, social media, analysts and technology vendors, new scams and fraud attacks - is overwhelming, to say the least. For mature banks, any change can only move as fast as an aging, siloed, technology stack. Tomorrow's risk is cancelled out by today's chance of potential operational downtime and disappointing customers. Younger banks appear more fearful of existential threats driven by regulation, embracing new technology to protect their customers.

Working with research firm Censuswide, Mitek surveyed 1,500 risk and innovation leaders in the financial services sector from Europe and North America[1]. They shared their insights on how the identity landscape is changing, the hurdles they face, and the tools they use and need to fight fraud.

Facing the fear of the unknown

The velocity of change has created a growing knowledge gap, feeding fear of the unknown for banking leaders. Banks care deeply about their customers. They are investing millions of dollars into getting to know and protect them. However, just over one-third (34%) of banks today told us they struggle to prove the identity of their customers.

Technology investments can only move the needle when banks have an optimal process in bringing all customer interactions, past and present, into one, clear view.
What's more, 76%[2] of banks told us fraud cases and scams have become more sophisticated. We see accounting for billions lost to fraud in 2023, with more than half a billion pounds in the UK[3] , $8.8 billion in the US[4] , and €1.8 billion in Europe[5]. And it's not going to get easier for banks – or their customers – to fight ever more sophisticated fraud.

Banking risk leaders told us the rise of Artificial Intelligence (AI) generated fraud is their top concern currently in their roles (37%). Despite acknowledging the need to do more, not all banks can move at the pace required to confidently tackle these current and emerging challenges.

Yet, there is hope

Banks, young and mature, understand they can become even stronger than before. What they are asking for, to build their confidence in meeting their customers' needs, is the ability to see around corners. The financial services sector cites three needs to prevent fraudsters from succeeding:

- Deeper understanding of the latest regulations (36%)
- Reduce technological complexity (36%)
- Be able to respond in real-time to customer requests and intelligence on what customers could do next (36%)

Banks have an opportunity to collaborate with technology vendors and partners to develop their identity lifecycle strategy and create a blueprint for success.

34%
of banks today told us they struggle to prove the identity of their customers

76%
of banks told us fraud cases and scams have become more sophisticated

37%
AI-Generated fraud is their top concern currently in their roles

[1] Risk and innovations leaders surveyed were from the UK, Spain and USA. [2] "a great deal" and "somewhat" answer options combined. [3] UK Finance [4] The Hill [5] Politico

Letting your real customers in

Letting your real customers in

We only open our front door to people we trust — but how do we know who is there? We get to know our neighbors, the cars people drive, what time they come and go. We notice patterns in behavior and notice when something is unusual.

Similarly, banks, who we trust to keep our money safe, are always looking to understand their customers better. They invest in and deploy technology that captures data points from various channels on how people engage with and access their finances. This data helps banks to form patterns which are used to identify and better serve their real customers while detect fraudulent behavior effectively.

Do banks know who their customers are?

Some banking leaders believe their organizations are not currently doing enough to know their customers. Just over a third (34%) cite knowing or proving the identity of customers as a challenge in their role. Looking to the next five years, this statistic hardly changes (33%). Complying with the Know Your Customer (KYC) regulation is an ongoing challenge and highlights the need to continually review processes.

To fully know their customers, banks must identify who they are and monitor their intentions. Banks cited customer onboarding, or account setup, as where they see the most fraud (42%)[6] and the most risk (41%). Identifying customers at this stage is critical for safety.

Worryingly, 1 in 6 (18%) banks find it hard to identify customers at any stage of the customer journey, stressing the importance of creating a holistic identity lifecycle strategy.

1 in 6

banks find it hard to identify customers at any stage of the customer journey

Fraud and scams are becoming fancier

More than three-quarters of banks believe that fraud and scams have become more sophisticated (76%)[7]. The majority of risk professionals told us they suspect up to 30% of all transactions could be fraudulent. Banks fear their abilities to both know the right person and keep the bad ones out.

When asked for their top concerns currently in their roles as risk leaders, the highest concern was AI-generated fraud and deepfakes on the rise (37%). Deepfakes are digitally altered videos of a person where they appear to be someone else.

Banks should rebuild their defenses for the future

When looking at current threats and those in the next five years, the one concern that remains consistent is escalating AI-generated fraud and deepfakes – with one distinct difference, timing.

- More mature banks, over 50 years old, count deepfakes as a current fraud threat (23%), but not as much in the future (18%).
- For fraud, the youngest banks, up to 10 years old, are the most concerned of any bracket (34%) when looking to the next five years, and the least intimidated currently (18%).

Today, mature banks have technical challenges to overcome so they can rapidly respond to current fraud risks. Yet, when looking into the future, they have more experience handling fraud threats, so they seem more optimistic, while younger banks lack this experience and are more worried about what developments lie in wait.

[6] "during customer onboarding" and "during customer onboarding and after onboarding" answer options combined

[7] "a great deal" and "somewhat" answer options combined.

Last year, up to

30%

of all transactions were suspected fraud cases by 32% of risk professionals

Summary

- More sophisticated fraud requires agile solutions which can detect and resolve current and emerging threats such as AI-generated fraud
- Banks should rejig their threat priority list to match up with where they notice the most fraud
- Mature banks can level up legacy systems and build out a robust identity lifecycle strategy
- Younger banks must not let fear of the unknown undermine their ability to innovate

Customer success could lie in how well-equipped different banks feel to tackle fraud. Currently, mature banks may not have the infrastructure in place for rapid responses to emerging threats such as deepfakes, so rank it as a top concern.

The youngest banks, influenced by their survival instincts to uphold their burgeoning reputation and revenue, are naturally most fearful of any future fraud risk that could quickly lead to their demise.

> **CHRIS BRIGGS**
> SVP Identity, Mitek Systems

3

Drawing back the curtains for change in the banking sector

Drawing back the curtains for change in the banking sector

The core responsibility of banks is to keep customers, and their finances, safe. To do this effectively, financial services firms are investing in fraud prevention technologies and customer experience to make the entire customer journey secure and frictionless.

Is the financial services industry doing enough to protect their customers?

Most banks (85%) are confident they are providing adequate security for their customers. However, when looking at different ages of banks mapped against their confidence levels, it's a different story.

- Surprisingly, only 78% of respondents from banks over 50 years old feel they are doing enough today. This lack of confidence could stem from the complexity of their decades-old IT systems and difficulty weaving new identity verification technology into heritage systems while avoiding downtime.
- However, firms less than 50 years old are confident in their ability to protect customers; with 91% sure of their abilities. Younger banks or fintechs, perhaps free from the technology straitjacket of legacy banking systems, have more faith in their digital banking ecosystem.

When looking at different nations, US banks were least confident in their ability to protect customers. Only 78% of respondents believe they are doing enough, while Spain and UK banks proved more confident with 90% and 88% respectively.

This confident outlook in Europe could be linked to directly operating within the region where these global identity, data protection and AI regulations are created. This places European banks under immediate scrutiny from lawmakers compared with their US peers, which accelerates the needs to act fast.

Where are banks investing?

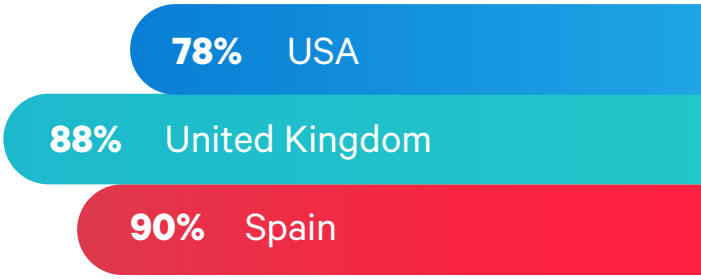
When asked about investment, leaders spent more on improving customer experience (CX) than they did on either fraud compensation or prevention. On average, innovation professionals at banks:

- Spent $3.5 million annually on improving the customer experience
- Invest $3.1 million each year in fraud prevention technologies

When looking at different maturities, older banks spent significantly more on CX ($3.9 million) than fraud prevention technologies ($3.1 million). Fintechs spent similar amounts on CX ($3.2 million) and fraud prevention technologies ($3.1 million).

Mature banks rank CX higher on their priority list — but may be forgetting that fraud prevention and better CX can go hand-in-hand. Fintechs ranked combatting fraud as a higher concern, investing relatively more on fraud prevention compared with mature banks, report lower suspected fraud cases and lower percentages making it through their defenses.

most banks surveyed feel they are doing enough to protect their customers



13%

More Fintech banks believe they are doing enough to protect customers compared with mature banks

Summary

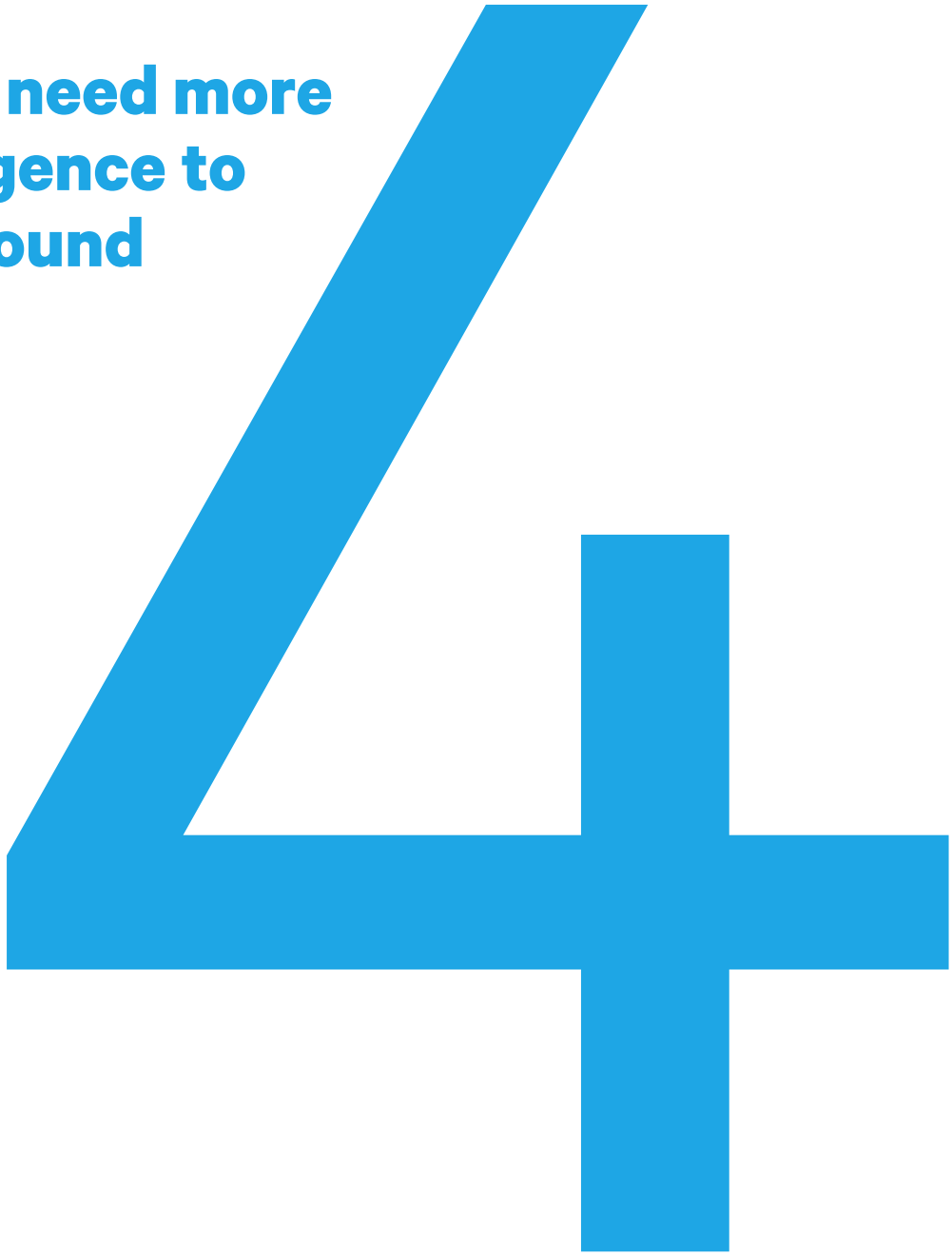
- Banks must fight the source and prevent fraudsters from slipping through the net. Ultimately, greater confidence in protecting customers hinges on innovation in fraud detection and prevention
- Mature banks can learn from their digital-native competitors by investing equally in both fraud prevention and customer experience enhancements
- Younger banks must not forget about customer experience in their quest to vanquish fraud and keep customers safe

Customer success could lie in how well-equipped different banks feel to tackle fraud. Currently, mature banks may not have the infrastructure in place for rapid responses to emerging threats such as deepfakes, so rank it as a top concern.

The youngest banks, influenced by their survival instincts to uphold their burgeoning reputation and revenue, are naturally most fearful of any future fraud risk that could quickly lead to their demise.

> **MARC SABARDI**
> Identity Innovation Lead,
> Mitek Systems

Banks need more intelligence to see around



Banks need more intelligence to see around corners

The desire for change is palpable. Financial institutions are futureproofing their revenues with customer experience upgrades and fraud prevention, however the research tells us they believe they can do even more.

Where are banks looking for help? Regulators? Technology vendors? Customers? We suggest: Identity intelligence.

Of those banks that felt they weren't doing enough to help protect their customers, these are the main focus areas they identified for improvement:
Deeper understanding of the latest regulations (36%)
With regulation taking the top spot, banks indicate concern that their current data protection and fraud detection methods may not meet regulatory requirements, especially when some rule makers are querying the use of artificial intelligence (AI) in biometric verification. Financial institutions (FIs) should see regulation as a strategic opportunity, and not a tick-box exercise.

Younger banks ranked this as their biggest growth area. This may point to newer fintechs being disproportionately affected by regulatory challenges compared with more established banks — and the survival of young banks may depend on navigating the regulations correctly.

A reduction in technologies, solutions, and vendors (36%)

The Identity market has seen consolidation in recent years. Research from Liminal indicates financial services enterprises prioritize speed, accuracy, and value for money from their vendors. More fintechs than mature banks cited this need to keep their technology stack simple to improve fraud prevention. A reduction in technology vendors can improve pace and security when moving from multiple-point solutions to a singular platform with many integrated components. Less is more.

The ability to respond real-time to customer requests (36%)

Financial services companies are trying to improve the customer experience by responding real-time. Older banks note that the ability to respond real-time to customer requests (37%) is the top area that requires improvement, which may explain their large investment in CX. It is possible today for banking innovators and risk professionals to balance CX with revenue. Speed AND security together at once. No compromises.

Intelligence on what their customers could do next (34%)

Staying one step ahead by understanding what the market needs, and then delivering the appropriate experience will enhance customer lifetime value for the financial services industry. This requires a strong understanding of macroeconomic forces at play today. One formidable risk that's currently threatening society is currency inflation which has made borrowing more expensive, fueling the global cost of living crisis. To make up for a shortfall and continue enjoying the same lifestyle, at-risk customers may turn to more perilous financial options, putting themselves and their FIs at risk. Intelligence will help banks make informed decisions to protect their most vulnerable customers.

More staff in their team (33%)

Although automation helps fill the void of technology staff shortage by reducing manual work, this does not entirely solve risk management. For instance, risk leaders were 1.4x more likely than innovation leaders to express a need to expand their teams, calling for new recruits to navigate legacy systems, provide manual checks, and bring fraud prevention technology up to scratch.

37%

of older banks note that the ability to respond real-time to customer requests is the top area that requires improvement

Summary

- Building customer intelligence brings benefits to fraud pattern detection
- Banks can have speed and security at once, no compromises. Rapid identity verification technology (IDV) enhancements can bring immediate, and future-proofed, results
- Mature banks should reprioritize their technology stack to take advantage of new weapons to fight fraud
- Younger banks mustn't live in fear of regulation but continue building the right technology infrastructure to navigate it

Banks should see regulation as an opportunity to implement technology that prioritizes protecting vulnerable customers from the threat of identity theft. This means following regulatory guidance on the adoption of technology and underlying data principles to reassure customers that their safety is the banks' top priority.

We recommend banks work with their technology vendors to confirm their product roadmaps align with regulatory standards, today and tomorrow. Having the right identity platform allows banks to be proactive and anticipate the constantly changing fraud landscape, which, in turn, protects the most vulnerable customers from the growing sophistication of fraudulent attacks.

> **GILLIAN CHANNER**
> VP Product Management,
> Mitek Systems

The blueprint for success

The blueprint for success

How banks, young and old, can learn from each other

The summary of this index highlights three key practical takeaways for financial institutions that recognize doing the same thing as before will not ensure customer lifetime value.

Mature banks recognize the need to innovate at the pace of change to reduce fraud and truly protect their real customers, while younger banks must persist with innovation in the face of changing regulation and emerging threats.

1. BE BOLD AND FAST

Banks should strike a balance between spending money on what they should do and what they can do. To move at the same pace as the market, leaders must not let the risk of the unknown or their monolithic technology stack limit their decision-making capabilities. Be bold and be fast; work with partners who facilitate agility and understand that every bank's ecosystem is unique.

2. SEE REGULATORY COMPLIANCE AS A GROWTH OPPORTUNITY

FIs should start viewing fraud prevention and regulatory compliance as long-term, strategic opportunities to differentiate and bolster their security. Compliance is more than a tick box exercise. To satisfy regulators, safeguard the customer experience, and stand toe-to-toe with fraudsters, financial services organizations should have a clear picture of how much fraud there is and do the right things for the right reasons. Banks must constantly test the edge to balance both protecting the consumer while also identifying fraudulent activity.

3. SHIFT THE FRAUD PREVENTION STRATEGY FROM REACTIVE TO PREDICTIVE

Fraud prevention must focus on converting data into actionable intelligence. Look for anomalous usage patterns and alert users. See when and where fraud trends are spiking, and then turn up verification accordingly in that area or during that time.

Work with other banks to set up an identity intelligence ecosystem to share fraud threats real-time.
This ecosystem prevents criminals from jumping from one bank to the next to find and exploit the most vulnerable. Creating these fraud patterns can contribute to building one true image of each customer.

Aside from protecting the customer, this data may unlock unexpected customer experience benefits such as creating smoother digital experiences and providing real-time new service offerings based on where, how and when customers access their bank accounts.

Methodology

Mitek, in partnership with Censuswide, surveyed 1500 UK, US, and Spain leaders in the financial services sector. They were in the roles of head of risk and head of innovation in retail and corporate banking. Respondents worked for organizations with an average of 4.47 million customers. The survey fielding was conducted in January 2024 by Censuswide.

Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.

Maturity	No. Of respondents	Percentage of overall sample
up to 10 years	50	3%
10 to 20 years	305	20%
20 to 50 years	478	32%
50 to 100 years	494	33%
100 to 150 years	152	10%
Over 150 years	21	1%
Younger banks (0-50 years old)	833	56%
Older banks (50+ years old)	667	44%

Authors

Chris Briggs

SVP Identity

Chris leads Mitek's Identity business, the company's product strategy and development, R&D, go-to-market and engineering teams. Chris joined Mitek in 2022 and has been instrumental in driving product innovation and partnerships. Chris brings more than 25 years of experience deploying mission-critical products for global technology services, data, analytics and consulting firms including Equifax, Experian and Accenture. Chris' passion is protecting consumers and helping companies provide safeguards for sensitive data in an ever-evolving world.

Gillian Channer

VP Product Management

Gillian plays a strategic role in shaping and delivering the company's consumer identity solutions. She leads a global team of technologists and business experts, driving innovation to protect companies and consumers from the growing threats of fraud and other financial crimes. Prior to joining Mitek, Channer served as Chief Product Officer for Capita, a leading United Kingdom-based consulting, transformation and digital services business. Earlier, she held leadership roles at Oracle, most recently as Senior Director of Business Operations.

Marc Sabadi

Identity Innovation Lead

Marc spearheads transformative strategies in identity solutions in the European market with a keen focus on safeguarding against fraud and enhancing user experiences. Prior to Mitek, Marc honed his expertise at companies like Paack and Aureo, specializing in B2B sales and technology solutions. Marc holds an MSc in Local Economic Development from the London School of Economics. Marc brings a unique perspective to the forefront of identity innovation.

Angela Romei

Corporate Communications Director

Angela leads the global corporate communications and public relations program. She designs the approach which keeps Mitek front and center in the identity verification category. Using strategic messaging, Angela positions Mitek as the layer of trust that every business needs, now more than ever - to keep their customers' data safe and secure. An expert in the art and science of connecting people with brands to drive business impact, Angela's twenty-plus years of experience includes Nike, Microsoft, Avanade and Accenture.

Mitek

About Mitek Systems

Mitek (NASDAQ: MITK) is a global leader in digital access, founded to bridge the physical and digital worlds. Mitek's advanced identity verification technologies and global platform make digital access faster and more secure than ever, providing companies new levels of control, deployment ease and operation, while protecting the entire customer journey. Trusted by 99% of U.S. banks for mobile check deposits and 7,900 of the world's largest organizations, Mitek helps companies reduce risk and meet regulatory requirements. Learn more at miteksystems.com.

Follow us

and read Mitek's latest blog posts here: miteksystems.com/blog