



Experian's 2025 U.S. Identity & Fraud Report

Traversing trust, technology, and the shifting identity landscape



CONTENTS

01

NEW ACCOUNTS:
FEWER OPENINGS,
HIGHER
EXPECTATIONS

07

CONCLUSION:
TRUST AS A
STRATEGIC ASSET

16

FOREWORD

02

BUSINESSES:
CONCERNED,
CONFIDENT BUT
NOT COMPLACENT

09

HOW EXPERIAN
CAN HELP

18

DIGITAL RISK IN A
FLUID ECONOMY

03

THE AI PARADOX:
HYPE, HOPE AND
HESITATION

12

FRAUD TAKING AN
EMOTIONAL TOLL

05

TRUST IS
SHIFTING—AND
FRAGMENTING

14



FOREWORD

ABOUT THE RESEARCH

The 2025 Experian Identity & Fraud Report marks the 10th year of the study. The report is based on two major surveys conducted in the U.S. in March and April 2025. The first asked more than 2,000 U.S. consumers about their online interactions and expectations regarding security and customer experience.

Consumers surveyed were tiered by age range: 18–24, 25–39, 40–54 and 55–69, and also by income level: below \$50,000 (low), \$50,000–\$99,999 (mid), and \$100,000 and above (high). The second survey asked more than 200 businesses in the U.S. about their strategies for effective fraud management, customer identification and authentication, including investments related to security and customer experience.

Companies ranged in size from \$10–\$49 million to above \$1 billion in revenue. Industries that completed the survey include retail banks, fintechs, consumer technologies and electronics, payment system providers, and many other companies from a range of verticals.

In today's hyper-digital economy, trust has become the currency of commerce — and it's under pressure. As we step into the second half of the decade, the stakes have never been higher. The convergence of increasing fraud sophistication, shifting consumer expectations and the proliferation of new technologies like generative AI is reshaping the identity landscape.

This year's report, now in its 10th year, is more than merely a study of fraud trends — it's a barometer of confidence for consumers and a strategic compass for businesses. Drawing insights from more than 2,000 U.S. consumers and 200 businesses, the findings reveal a marketplace that's simultaneously optimistic and anxious, connected and fragmented, empowered and vulnerable.

It's this type of tumult that creates an opportunity-rich environment for fraudsters. Amid this continuously expanding risk landscape fraught with more complex fraud implications, key questions remain for both consumers and businesses:

- How secure do consumers feel online, and how have their security and experience expectations changed in the last year?
- Are businesses increasing investments sufficiently to tackle growing fraud challenges?
- Do they have effective technology solutions in place to accurately identify and authenticate consumers?
- How is GenAI impacting consumers and businesses in the fraud landscape of 2025?

As you read this report, consider it a lens not just on where we are but also on where the market is headed — and what it will take to lead with confidence in a world where identity is both an asset and an attack vector.

Armed with this insight, together, we can help you shape the next-generation fraud and identity strategies that will protect your business and consumers in 2025 and beyond.



Kathleen Peters
Chief Innovation Officer
Experian North America

Digital risk in a volatile market landscape

For years, the prevailing wisdom has been that fraud would increase along with digital adoption, and 2025 confirmed that trend. Fraudsters chase opportunities, and ongoing economic and political instability continue to provide a fertile ground for malicious actors. In fact, the FTC’s latest report shows that in 2024, fraudsters exploited every chance to scam consumers, with U.S. consumers reporting over \$12.5 billion in losses — a 25% rise from the previous year.¹ The FBI also reported a record \$16.6 billion lost to scams and cybercrime in 2024, a 33% increase from 2023.² Our research indicates that U.S. businesses are feeling the impact too, with nearly 60% reporting higher fraud losses compared to the year before. Not only have losses surged, but the tactics behind them have also changed significantly.

Fraudsters, emboldened by new technologies and systemic vulnerabilities, are getting faster, smarter and better able to scale their crimes. Deepfakes and real-time social engineering are no longer fringe tactics; they’re mainstream tools in fraudsters’ playbooks. Against this backdrop, consumer anxiety is holding steady. While 57% of consumers report being concerned about online activity — up from 51% last year — that number is lower than prior highs. Is this resilience or resignation?

Table 01: Consumer concern about online activity (2022 - 2025)

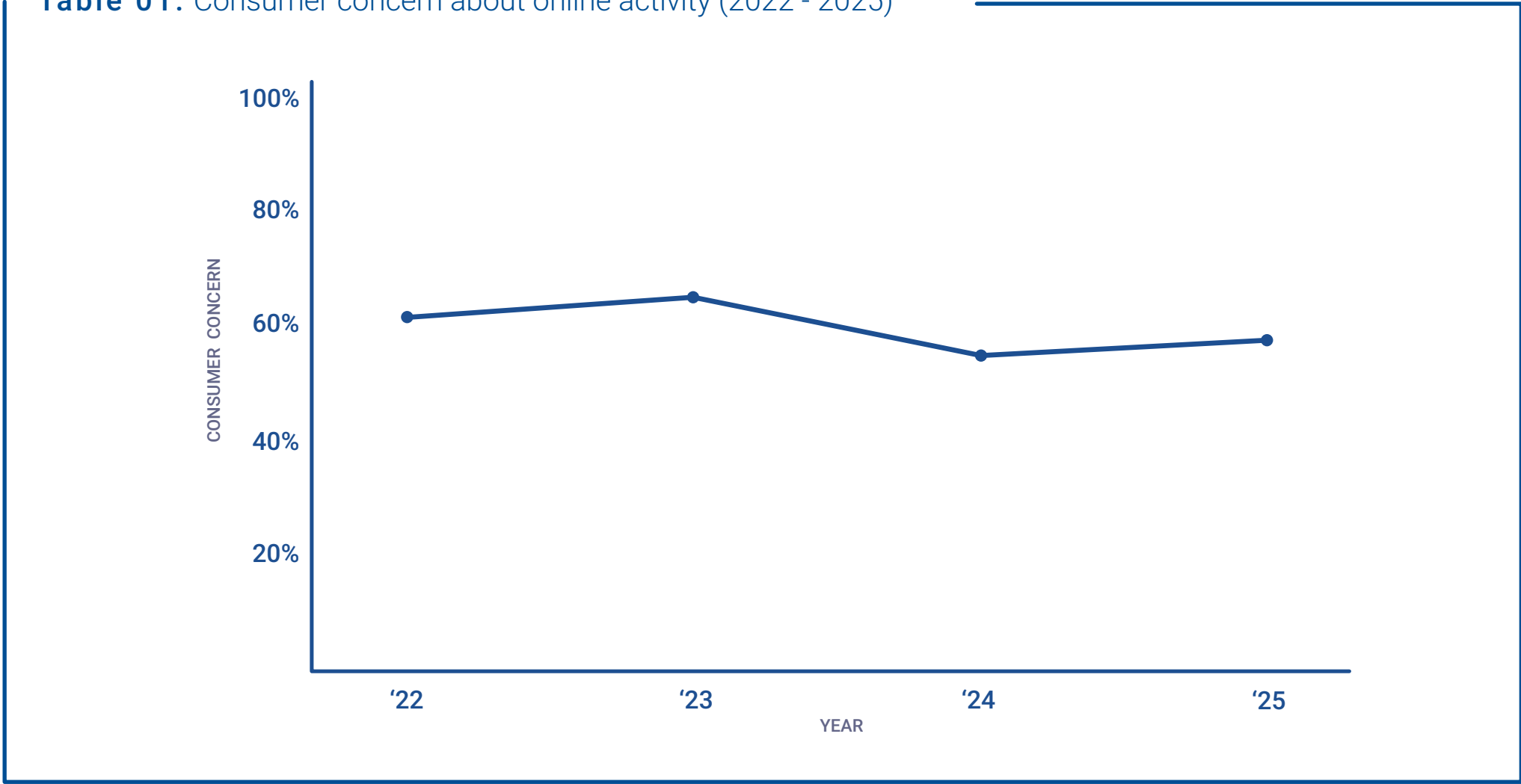
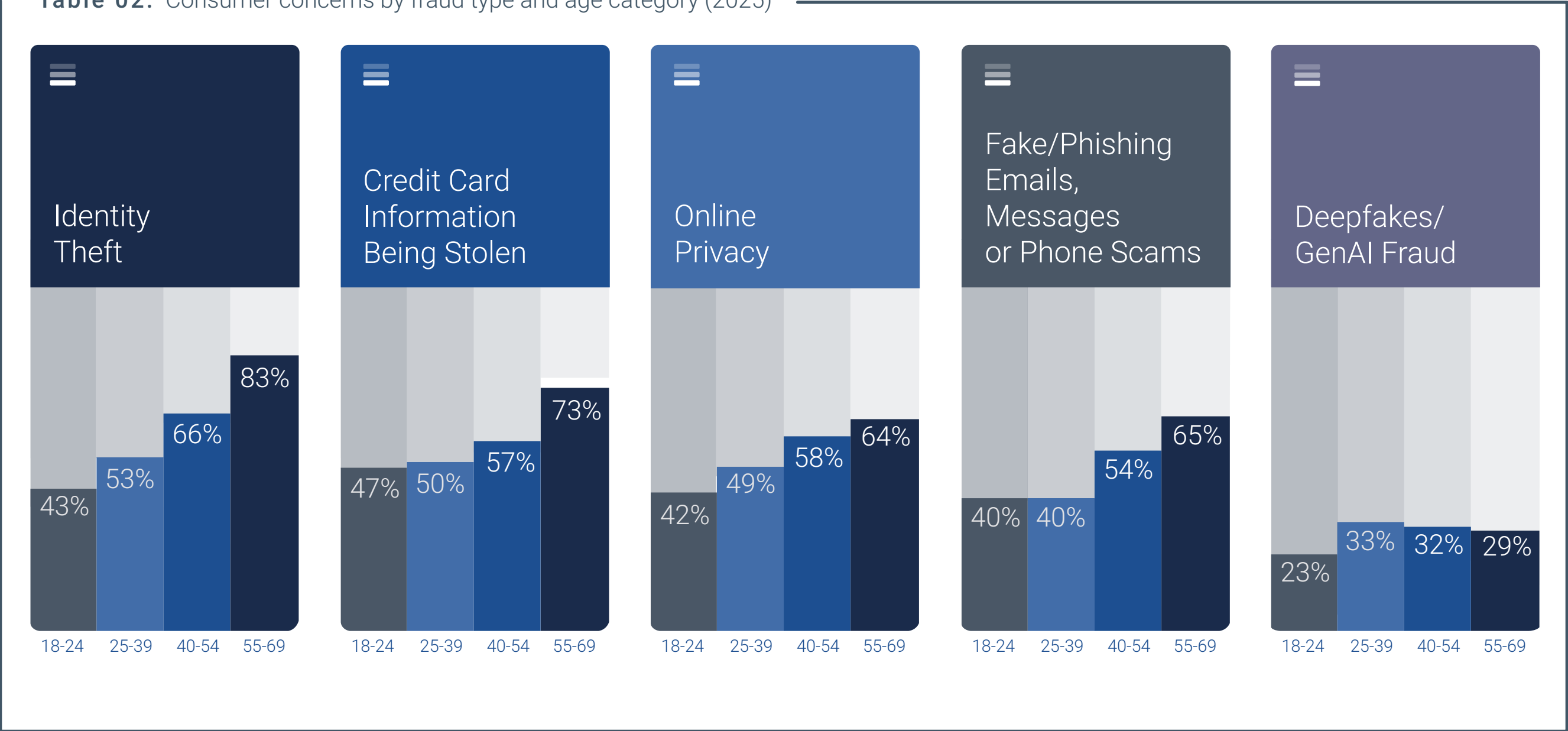


Table 02: Consumer concerns by fraud type and age category (2025)



A closer look reveals deeper nuance. Digital natives aged 25–39 show the highest concern, not despite their fluency with technology, but because of it. They understand the risks intimately, and they know that even “smart users” aren’t immune. Meanwhile, high-income households, more likely to engage in mobile banking, P2P payments, and crypto transactions, are grappling with a rising number of touchpoints and exposures.

Yet, digital behavior continues to surge. It seems consumers aren’t retreating, they’re recalibrating. They expect security to be proactive and integrated. They want reassurance, not restriction. The challenge for businesses? Design systems that anticipate these demands without introducing friction.

In a landscape defined by fluid risk coupled with rising expectations, identity isn’t a checkpoint — it should be viewed as a dynamic trust contract, renewed with every interaction.

¹ <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>
² <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>

Fraud taking an emotional toll



When we talk about fear in the digital marketplace, identity theft still reigns supreme. This year’s research reveals that 68% of consumers place it at the top of their online security concerns, with stolen credit card information (61%) not far behind. These numbers are more than statistics — they’re reflections of a growing emotional reality: Consumers are tired of feeling exposed.

More than that, research shows the impact of fraud is taking an immense emotional toll on consumers. A recent report from the Better Identity Coalition found that of the victims reporting into the Identity Theft Resource Center (ITRC), 96% report emotional impact, such as shame, anxiety or depression. Even more alarming, 12% considered self-harm or suicide.³

Consider the 55–69 age group. They were thrust into the digital economy during the COVID-19 pandemic with no signs of going back. For many of them, the internet is both indispensable and a mystery — a place where their financial lives unfold, but where they also feel uniquely vulnerable. For younger consumers, particularly those between 25–39, the fear isn’t necessarily of being targeted — it’s being unknowingly manipulated, surveilled or impersonated. Their expectation of identity protection extends beyond fraud alerts; it encompasses digital autonomy, reputational integrity and control over personal data.

That’s why it’s interesting that the 2025 data also shows a subtle but important rebound in consumer openness to sharing their data. The percentage of consumers “very willing” to share personal data has ticked up to 16%, after bottoming out at just 9% last year.

What changed? Transparency. When businesses clearly explain why they’re collecting data — and how it will protect or benefit the customers — people listen. They’re not demanding perfection; they’re demanding honesty and clarity. Consumers are also more educated about the power of their data to help identify and protect them online. And they’re willing to work with businesses they trust to ensure their safety and positive experience online. We’re entering an era where trust won’t be granted based on brand name alone. It must be earned continually through simple, secure and respectful interactions. Every form fill, every authentication prompt, every fraud alert — these are moments to build or break confidence.

Table 03: Consumer willingness to share personal data (2022 - 2025)

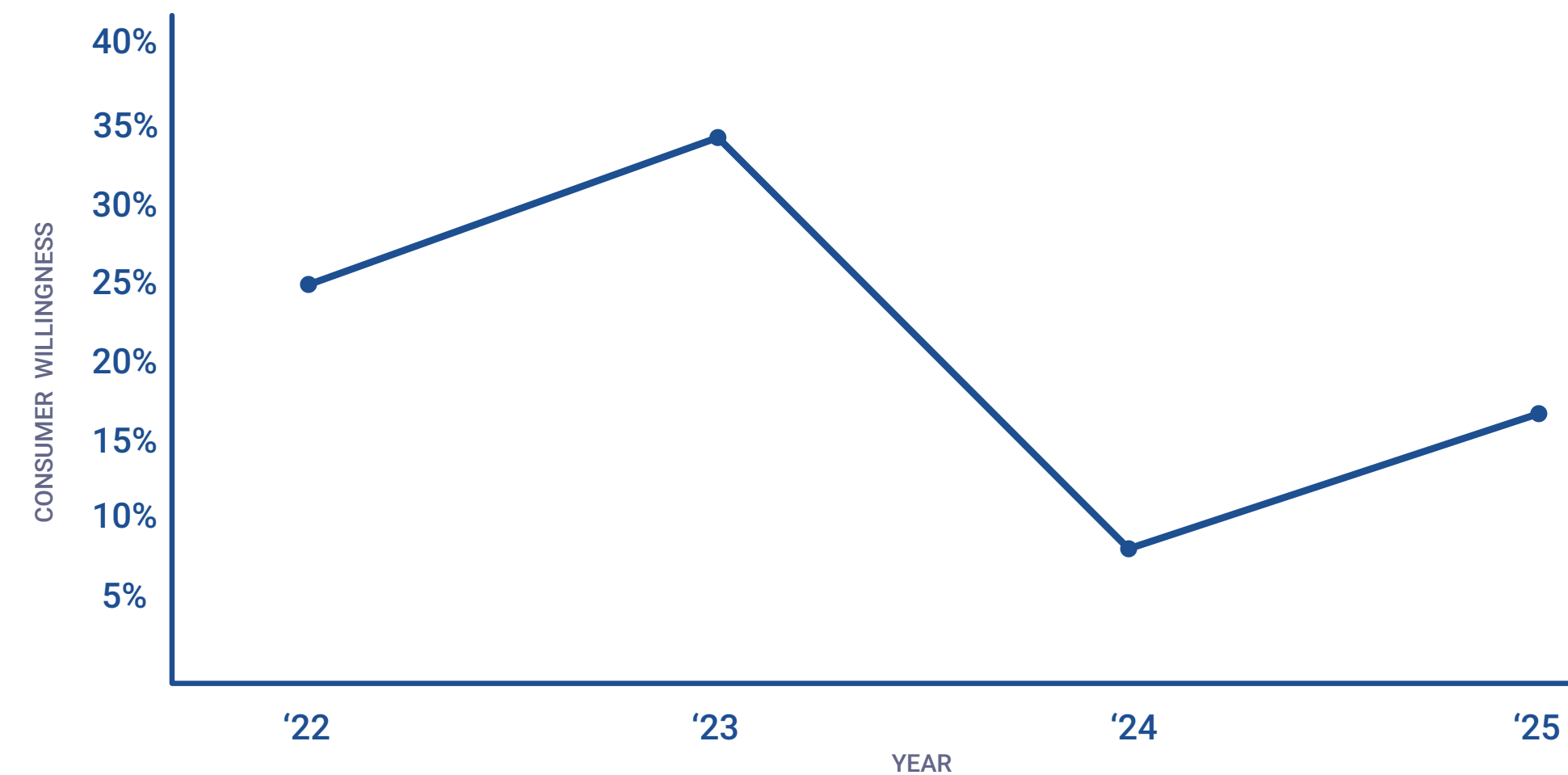
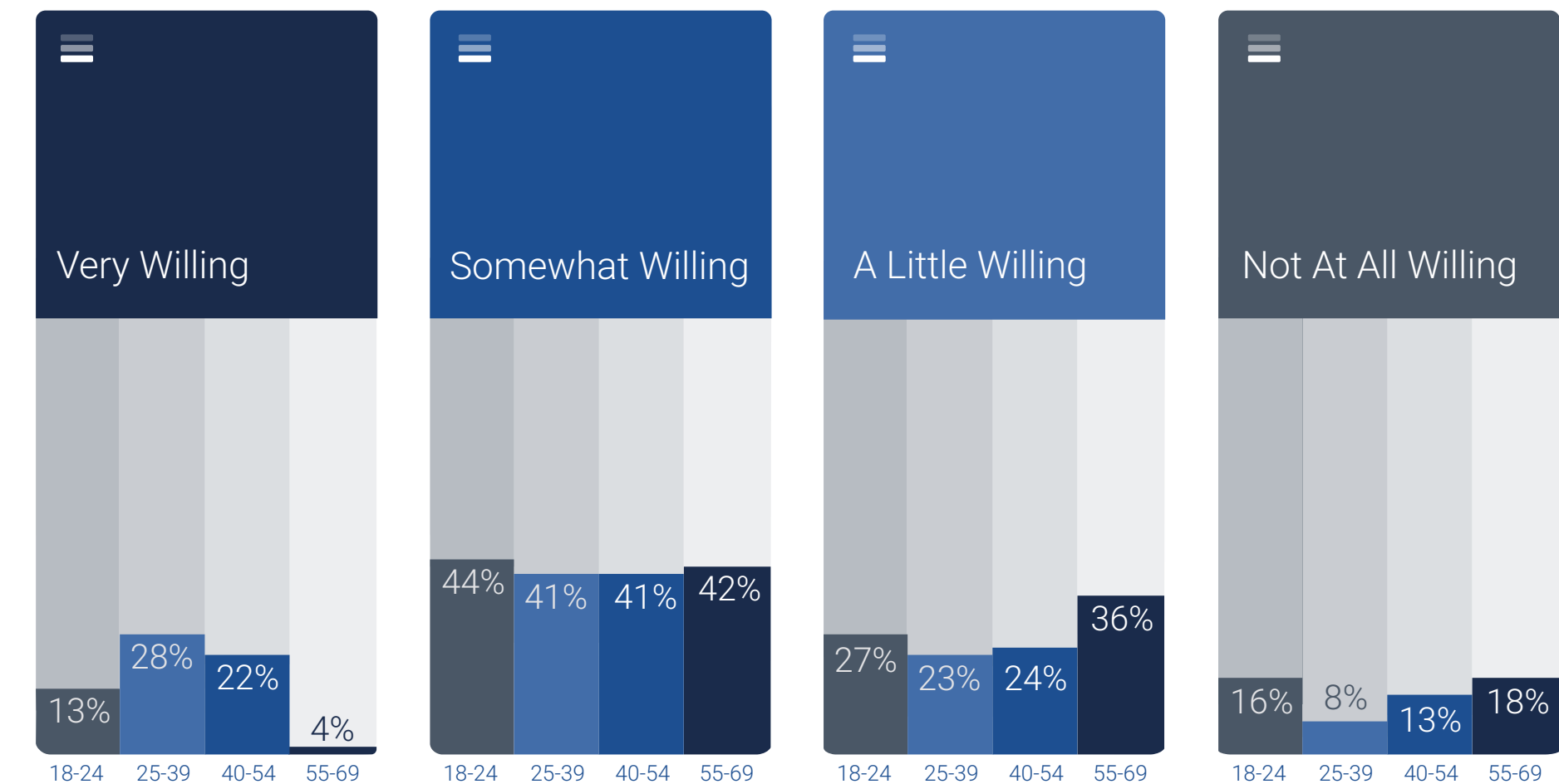


Table 04: Consumer willingness to share personal data by age category



³ <https://www.idtheftcenter.org/wp-content/uploads/2024/10/ITRC2024ConsumerandBusinessImpactReport.pdf>



New accounts:
fewer openings,
higher expectations

While consumer trust showed signs of recovery and digital activity soared, new account openings remained flat in 2025. Just 40% of respondents reported opening a new account in the past six months, a continuation of the downward trend from 2023. But the story isn't just about quantity — it's about quality.

Today's consumers may be signing up for fewer new services, but they're placing higher demands on every digital interaction. Four in 10 U.S. consumers said they considered abandoning a new account set up midway through the process, a figure that climbs to 50% among high-income earners and 45% among those aged 25–39. These groups are digitally active and brand-conscious, making them especially sensitive to poor user experiences.

What's behind this impatience? Partly, it's cognitive overload. Consumers are bombarded with logins, verifications and security protocols every day. But more fundamentally, it's about alignment. People expect onboarding to mirror the rest of their digital lives — fast, intuitive, personalized. This isn't just for companies with which they have existing business, but also new accounts with new businesses. They don't just want to be authenticated; they want to feel recognized.

Unfortunately, many companies are still stuck in the loop of legacy verification methods. Passwords, PINs and security questions are ubiquitous but less secure. Meanwhile, consumers view biometrics — both physical and behavioral — as more secure and seamless. However, they remain underutilized by businesses in account creation flows.

Our research shows that a negative onboarding experience not only leads to considerations of abandoning the process, but these thoughts also lead to action. Of the 40% of consumers who considered abandoning a new account opening, 52% actually followed through, choosing a competitor instead. The resulting message is clear: First impressions matter. If a brand fails to deliver a smooth, secure and confidence-inspiring experience during the first five minutes of interaction, that failure can reverberate for years.



40%

of consumers considered abandoning a new account opening due to a negative experience.

+

50%

of those consumers actually followed through, choosing a competitor instead.

Businesses:
concerned, confident,
but not complacent

If fraud lurks in the shadow of digital transformation, then 2025 marks a year when many businesses are shining a brighter light on it. Interestingly, even in the face of growing fraud threats, many U.S. businesses remain in growth mode, with 59% of respondents saying they are prioritizing revenue over fraud detection. Nonetheless, it's clear fraud is recognized as a critical business issue, with 90% of U.S. businesses reporting high or medium concern about fraud. Moreover, a full 96% of surveyed organizations say they understand fraud's impact, and 70% are increasing their fraud prevention budgets.

On the surface, this is progress. Beneath it, though, is a more complicated truth: Understanding doesn't always translate into preparedness. Even with increased understanding and awareness, nearly 60% of U.S. businesses reported increased fraud losses compared to the previous year. Respondents described a variety of fraud types causing concern, nearly in equal measure, including identity theft (39%), P2P payment scams (37%) and first party fraud (35%).

There are a host of factors driving fraud losses for U.S. businesses, but a critical issue is legacy security tools. Despite their intentions, many businesses still default to the tools of the past. Passwords, PINs and security questions dominate the authentication landscape — methods familiar to consumers, yes, but also increasingly viewed as frustrating and fallible. Meanwhile, more secure and user-preferred methods — such as biometrics and passive behavioral analytics — remain underutilized, often delayed by budget, complexity or inertia.

Here lies the contradiction: while 85% of businesses believe their fraud controls align with consumer expectations, less than half of people are highly trusting of companies to address their concerns online. Furthering the disconnect, our research shows that 57% of consumers are still concerned about doing things online, just 32% say businesses clearly explain data collection, and only 13% feel fully secure using a new brand. That's not a small gap — it's a credibility chasm.

But within this disconnect lies opportunity. The organizations that close this gap won't just reduce fraud — they'll unlock loyalty. Because today's consumer is watching closely, they notice when onboarding is easy. They reward brands that treat identity not just as a liability to be defended but as a privilege to be safeguarded. That reward comes in the form of trust, with 40% of U.S. consumers saying they're extremely or very trusting of businesses that can accurately identify and authenticate them on a repeated basis.

In navigating a shifting identity landscape, meeting consumers' expectations for security and identity authentication is more than a technical function. It should be your brand promise.

Table 05: Credibility gap between business and consumer confidence in fraud controls

85% of companies say they're confident their fraud controls align with consumer expectations



57% of consumers are still concerned about doing things online



32% of businesses clearly explain data collection



13% feel fully secure using a new brand



Table 06: Top 5 encountered fraud events by U.S. businesses

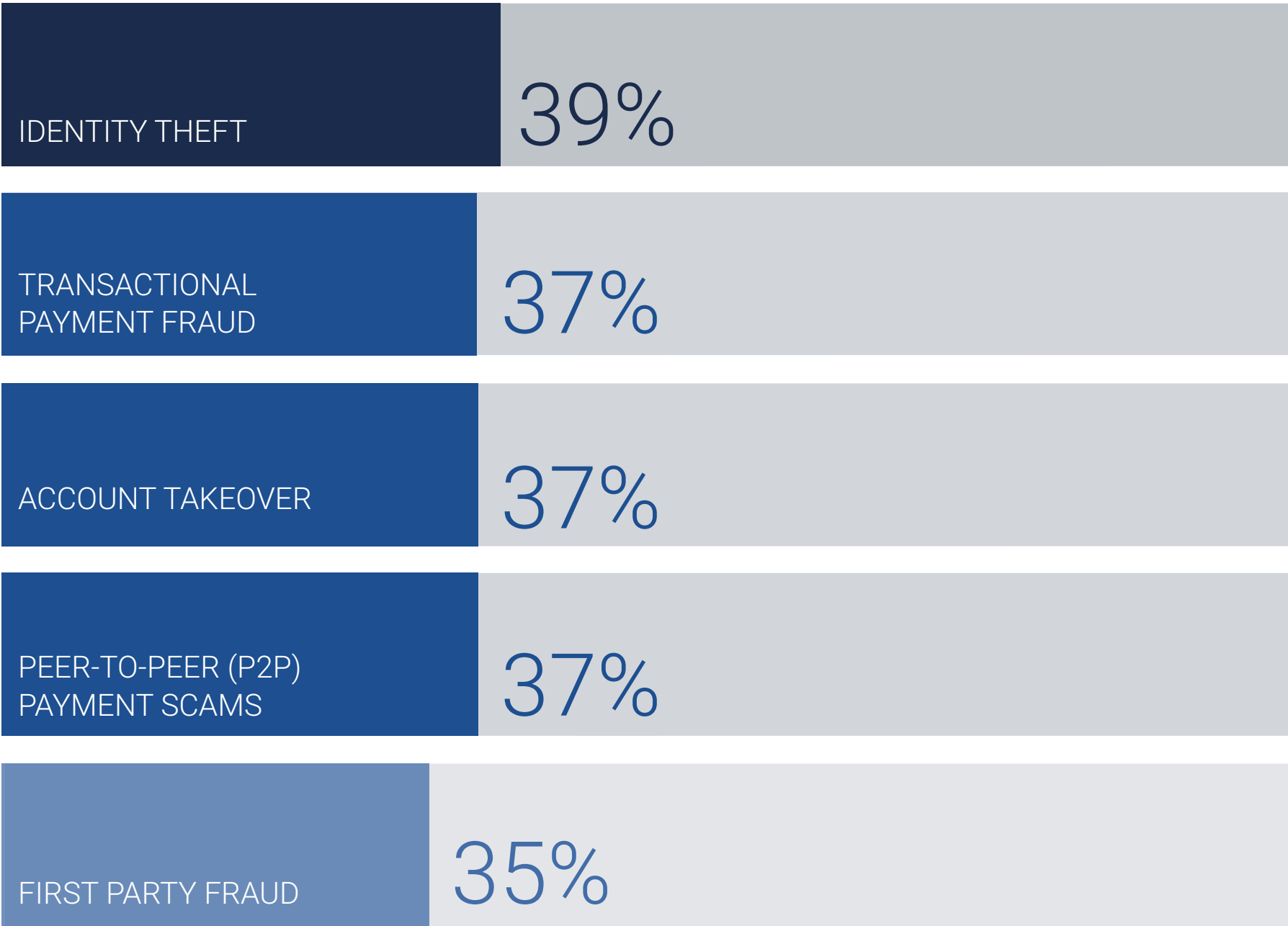
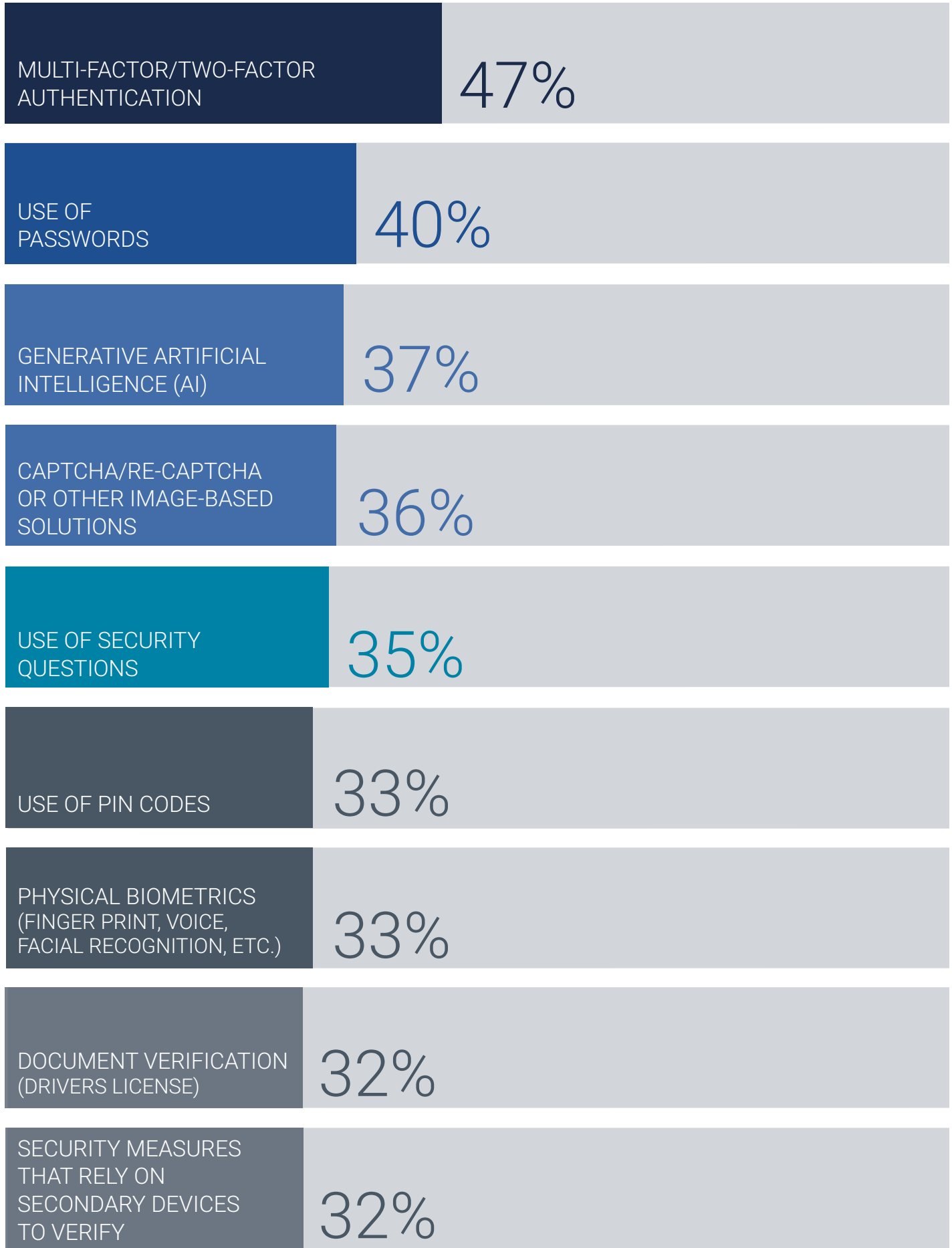


Table 07: Top fraud prevention methods used by U.S. businesses



The AI paradox: hype, hope, and hesitation

AI has emerged as both a savior and a saboteur in the fraud ecosystem. On one hand, GenAI is giving rise to synthetic fraud, convincing deepfakes and impersonation scams that are almost indistinguishable from real interactions. On the other hand, AI is the very technology that can help businesses detect anomalies, flag suspicious behavior, and preempt threats with greater speed and scale than ever before.

The rise of agentic AI — systems capable of autonomous decision-making and goal pursuit — adds a new dimension to the AI paradox. These agents can streamline financial operations, automate fraud detection and enhance customer service with unprecedented efficiency. But the same autonomy can be exploited by fraudsters to scale social engineering attacks, deploy adaptive scams or malicious bots, or even orchestrate multistep fraud campaigns without human oversight. As agentic AI becomes more accessible, the line between innovation and exploitation grows thinner. Businesses must not only adopt these tools but also build in safeguards, oversight and ethical guardrails from the start.

This paradox isn't lost on the market. While 72% of business leaders expect AI-generated fraud and deepfakes to be among their top operational challenges by 2026, and 63% feel confident in their ability to mitigate them. However, only 37% of businesses said they are currently using GenAI to detect and protect against fraud. AI use is rising, though, in other operational areas, including both internal and customer-facing applications; 55% of companies said they were implementing new AI methods and models and 52% focusing on fraud and customer decisions. It's clear U.S. businesses now consider AI a dual-purpose priority. It's both enhancing internal processes and improving customer interactions. Perhaps unsurprisingly, fintechs (64%) lead in AI for customer decisioning. In looking at the rest of the year, businesses are doubling down on AI tools that improve customer experience and combat application fraud. This is especially true among Tier 1 businesses overall and click-and-mortar retailers.

Consumers, meanwhile, remain cautious. Less than 1 in 4 report interacting with AI-driven tools like chat bots, and just 18% “completely trust” these tools. There’s a trust gap here — not in the capability of the technology, but in its intent and transparency. People want to know how AI is being used. Who’s training it? What data is being fed into it? What happens when it makes a mistake or has a hallucination?

To earn public trust, businesses must do more than adopt AI. They must educate, disclose and design with empathy. AI should be invisible when it works well, but always accountable when it doesn't. The companies that strike this balance will not only outpace fraud — they'll earn reputational capital in a world desperate for digital clarity.

72%

of business leaders expect AI-generated fraud and deepfakes to be among their top operational challenges by 2026.

Only

37%

are currently using GenAI to detect and protect against fraud.



Trust is shifting – and fragmenting



Table 08: Top Trusted Financial Entities

PEER-TO-PEER (P2P) PAYMENT APP	28%
CREDIT BUREAUS	28%
AUTO MANUFACTURERS	27%
PEER-TO-PEER (P2P) LENDING	27%
STREAMING SERVICES	26%
PAYMENT SYSTEM PROVIDERS	25%
RETAIL BANKS	24%
BUY NOW, PAY LATER PAYMENT FINANCING	24%
ONLINE GAMBLING COMPANY	21%
TECH PROVIDERS	21%



Consumer trust rebounded this year after a 10-20% decline across industries last year. This year’s results showed a bit of jockeying in the list of trusted entities, with P2P payment apps and credit bureaus each scoring 28%; auto manufacturers (27%), peer-to-peer lenders (27%), and streaming services (26%) rounded out the top five. However, these numbers are still notably low. It’s no surprise, then, that just 32% of consumers believe businesses clearly communicate how their personal data is collected or used.

Yet, expectations remain high. More than 80% of consumers expect companies to act when they express security or privacy concerns. This isn’t a call for perfection—it’s a demand for presence, for visibility. For a sense that someone is on the other end, listening and protecting.

We’ve entered a new era, one marked not by institutions, but by interactions. Financial institutions traditionally top the list of trusted entities, but it’s not something they should take for granted. To keep their customers’ trust, it should be earned incrementally and renewed continually through clarity, control and consistency.

The implication for businesses is simple, but often complex to execute: You don’t just need better security — you need better communication about that security. You need to show your work, explain your guardrails and create experiences that feel as protective as they are seamless.

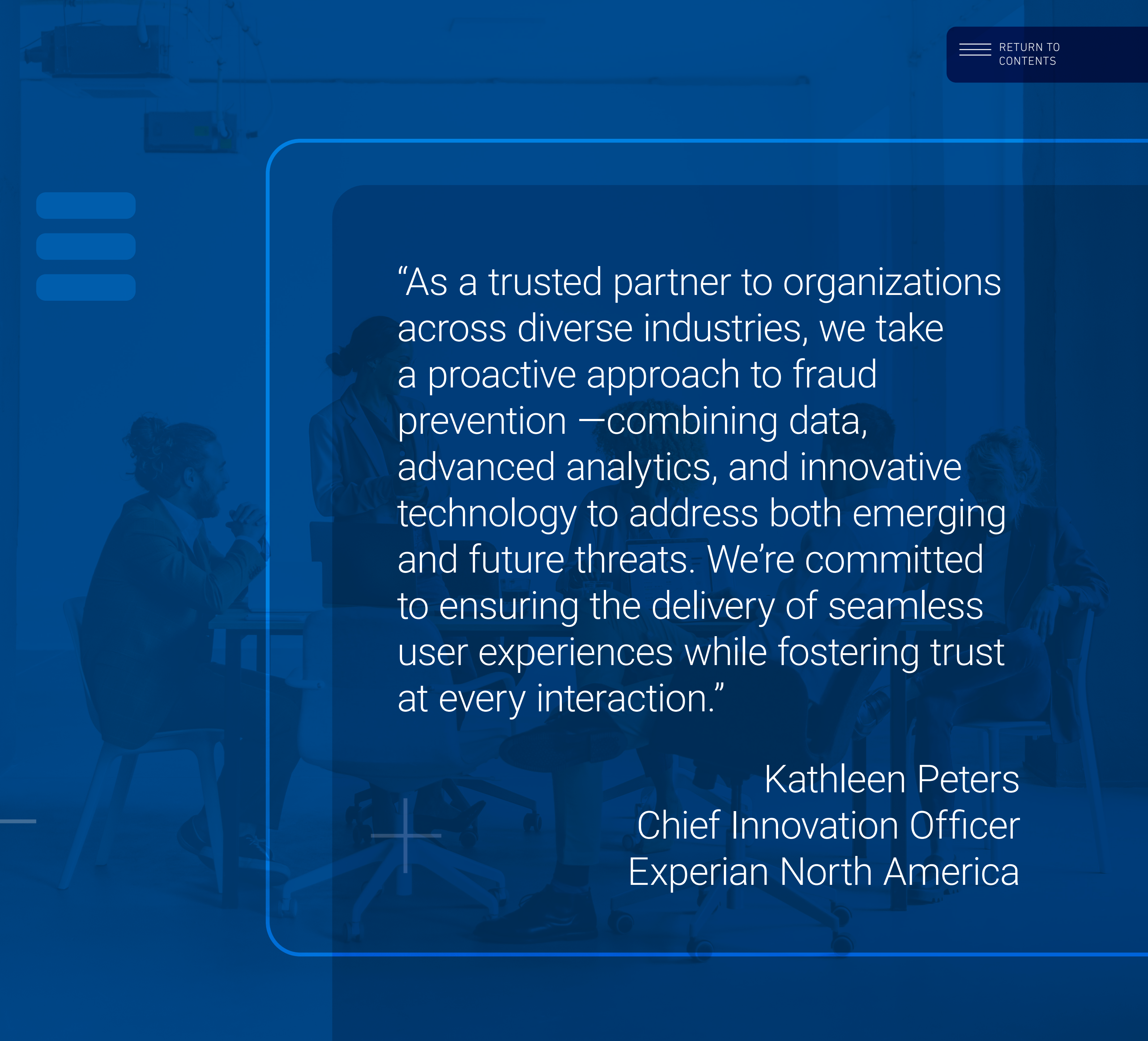
Today, trust isn’t just a brand attribute, and it’s more than a product feature. In 2025 and beyond, trust will be a business’s strategic asset.

Conclusion: trust as a strategic asset



The story of identity and fraud in 2025 is not just about risk — it's about **relationships**. In a digital world where consumers are both more empowered and more exposed, trust has become the defining metric of success. And businesses that recognize this will stop treating fraud prevention as a reactive cost center and start embracing it as a strategic asset.

Looking ahead, the winners in this space will be those who see the full picture — who recognize that identity isn't just about keeping the bad guys out. It's about letting the right people in, more quickly, intelligently and with greater trust than ever before.



“As a trusted partner to organizations across diverse industries, we take a proactive approach to fraud prevention — combining data, advanced analytics, and innovative technology to address both emerging and future threats. We're committed to ensuring the delivery of seamless user experiences while fostering trust at every interaction.”

Kathleen Peters
Chief Innovation Officer
Experian North America

How Experian can help

Comprehensive real-time identity verification and fraud risk detection

With the rise in digital account activity paired with increasing fraud threats, organizations need the right tools to stop fraudsters at account opening — without compromising the customer experience. Experian empowers businesses with advanced, real-time identity verification tools that assess risk at every touchpoint. By leveraging a vast network of data and machine learning models, we help detect and prevent fraud before it impacts operations or customers. Our layered approach — combining device intelligence, behavioral analytics and identity proofing — ensures that legitimate users are quickly verified while suspicious activity is flagged for further review. This comprehensive identity verification not only protects your business but also enables you to verify more consumers, recognize them consistently, and ultimately expand your portfolio and increase revenue.

Highly predictive fraud analytics

Experian's fraud analytics harness the power of data and AI to identify threats before they materialize. Our models are trained on billions of data points, enabling businesses to detect subtle patterns and anomalies that signal potential fraud. These insights help prioritize high-risk interactions and allocate resources more effectively to provide the right treatment at the right time. The result is faster decision-making and stronger fraud prevention without compromising customer experience.

Holistic identity theft prevention

We take a comprehensive approach to identity theft prevention that spans both proactive and reactive measures. Experian integrates identity monitoring, breach detection and recovery support to protect consumers at every stage. For businesses, this means fewer downstream impacts from compromised identities and greater customer trust. Our holistic strategy ensures that identity protection is not just a feature, but a foundational element of digital safety.

Compliance that provides a highly protected customer experience

Experian helps businesses navigate complex regulatory environments while delivering a seamless customer journey. Our solutions are designed to meet global compliance standards, including KYC, AML and data privacy regulations. At the same time, we prioritize user experience by minimizing friction through intelligent risk-based authentication. This balance of security and convenience builds loyalty and reduces abandonment across the customer lifecycle.

Fighting fraud with behavioral analytics

Behavioral analytics adds a powerful layer of intelligence to fraud detection by analyzing how users interact with digital platforms. Experian's solutions, powered by NeuroID, monitor keystrokes, navigation patterns and device behavior to distinguish between legitimate users and fraudsters in real time. This continuous authentication approach enhances security to fight third-party fraud and emerging fraud threats, such as next-gen bots, identity theft, account takeover and more, without disrupting the user experience. Tracking how every user interacts with your digital forms reveals their intentions in real time, so you can respond quickly. Our capabilities provide a seamless, invisible gauge of user risk, without capturing additional personally identifiable information (PII). By understanding behavior, we can stop fraud before it starts — often without the customer even knowing.

At Experian, we've long believed that the best security is invisible when it works and unforgettable when it's needed. We're the world's leading global information services company, and we have a long legacy of providing award-winning fraud and identity solutions to protect companies and their customers.

Our solutions are used at some of the world's largest banks and financial institutions to identify potentially fraudulent customers and transactions and to ensure that action is taken in real time to prevent fraudulent payments being made. Last year alone, our solutions helped save \$19 billion in fraud losses globally. But more than that, we've helped businesses build relationships that are rooted in confidence, convenience, trust and security while helping consumers build better tomorrows.

And we would love to help you.

[Click here](#) to learn more.



Experian helped
clients save
\$19 BILLION
in fraud losses
globally last year.

