EXPERIAN'S 2026 U.S. IDENTITY & FRAUD REPORT

Navigating fraud, AI and the future of digital trust

2026

_CONTENTS

_FOREWORD

KEY FINDINGS AT A GLANCE

- **Fraud is causing financial strain.**
  Consumers are experiencing personal financial loss from fraud, while 60% of businesses report higher fraud losses than in previous years.
- **AI-enabled deception is rising.**
  Consumers are aware of AI-generated fake media, AI phishing, voice cloning and impersonation scams. Businesses identify AI-generated phishing as a leading AI-enabled fraud risk.
- **Identity is central to trust.**
  Consumers value accurate recognition, and businesses are expanding authentication and identity intelligence.
- **Security must feel proportionate.**
  Most consumers will complete additional security steps, but patience declines when friction feels unnecessary.
- **Data control is part of trust.**
  Consumers want more control over how personal information is used, especially in high-trust digital activities.
- **Agentic commerce is the next frontier.**
  AI-assisted purchasing is emerging, raising future questions about agent identity, authorization and accountability.

Trust has always been at the heart of every human interaction, and financial services is no different. Every account opened, payment processed, application approved, and transaction completed depends on confidence that people and businesses are who they claim to be.

Today, that trust is being tested in new ways. Artificial intelligence is creating new opportunities to improve fraud detection, identity verification and customer experiences. It's also enabling more sophisticated phishing campaigns, synthetic identities, deepfakes, voice cloning and impersonation attacks.

This year's findings point to a clear convergence between consumer expectations and business priorities. Consumers are embracing digital channels while expecting stronger protection, greater transparency and more control over their information. Businesses are responding with investments in fraud prevention, identity intelligence, adaptive authentication and AI-driven decisioning.

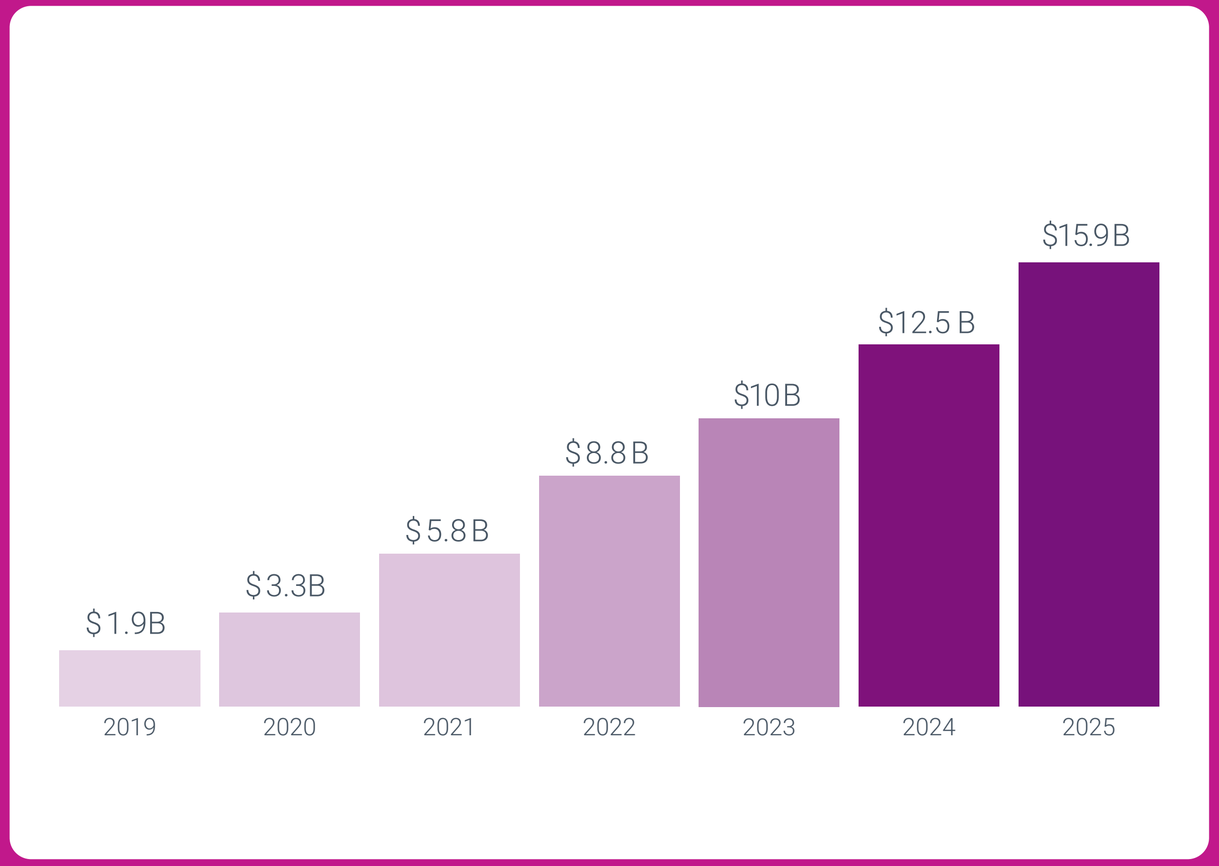
As we look ahead, the conversation extends beyond AI-powered fraud. Agentic AI and autonomous digital agents are poised to reshape the market, and AI agents will increasingly compare products, manage subscriptions, open accounts, schedule services and complete purchases on behalf of consumers.

The future of fraud prevention will depend not only on verifying people, but also on verifying the digital agents acting on their behalf. Identity, transparency and trust will become essential infrastructure in an increasingly autonomous digital economy.

Kathleen Peters
Chief Innovation Officer
Experian North America

_FRAUD BY THE NUMBERS

Table 01: U.S. fraud losses year-over-year growth



The FTC reported

$15.9 BILLION

in consumer-reported fraud losses in 2025.

Fraud continues to impose significant financial and emotional costs on consumers, businesses and institutions. Public reporting shows that fraud and cyber-enabled crime remain large and growing economic threats, although different sources measure different parts of the market.

The FTC reported $15.9 billion in consumer-reported fraud losses in 2025, based on 3 million fraud reports. That represents an increase of 32.5%, with more than $12 billion in reported fraud losses and 2.6 million fraud reports in 2024. The FBI Internet Crime Complaint Center (IC3) reported nearly $21 billion in cyber-enabled crime losses in 2025, reflecting a broader category that includes internet crime reported by individuals, businesses and institutions.

It's important to note that the FTC figure reflects consumer-reported fraud losses, while the FBI IC3 figure reflects reported internet crime losses, including categories such as investment fraud, business email compromise and tech support scams. Together, they point to the same conclusion: Fraud has become a large, persistent economic issue, and underreporting means the actual impact is likely higher.

Sources: FTC testimony on 2025 Consumer Sentinel reports; FBI 2025 Internet Crime Report

_CHAPTER 01

Fraud has become a persistent, multidimensional challenge

For years, fraud was generally observed as a singular event, a forged check, a stolen credit card, or an inflated invoice. But today's fraud landscape looks entirely different. For consumers, fraud or the attempt at fraud, is part of the background noise of digital life: suspicious texts, fake delivery notices, phishing emails, fraudulent ads and account-related alerts. For businesses, fraud has become a recurring, increasing operating pressure that affects losses, technology investment, customer experience and resilience.

This pressure is growing because digital participation keeps expanding. Consumers now use online channels for routine transactions, payments, banking, shopping, food delivery, account opening and customer support, reinforcing how deeply digital channels are integrated into daily life.

The consumer findings show that phishing and scam activity remain the most common fraud experiences. Among consumers who encountered fraud events in the past year, 26% cited fake or phishing emails, messages and phone scams. Other common events included false information or fake advertising, package delivery scams, credit card theft, unauthorized charges and fraudulent bank transactions.

The data also shows that fraud has both financial and emotional consequences. Nearly 1 in 5 consumers say they experienced financial loss due to online fraud in the past 12 months, and another 15% say fraud was attempted but prevented. Among victims, 72% say the experience made them feel more vulnerable.

That vulnerability can shape future behavior. Customers who feel exposed may become less willing to share information, less patient with unclear security steps and less forgiving when an organization appears slow to respond.

Table 02: Top fraud events encountered by consumers by income level

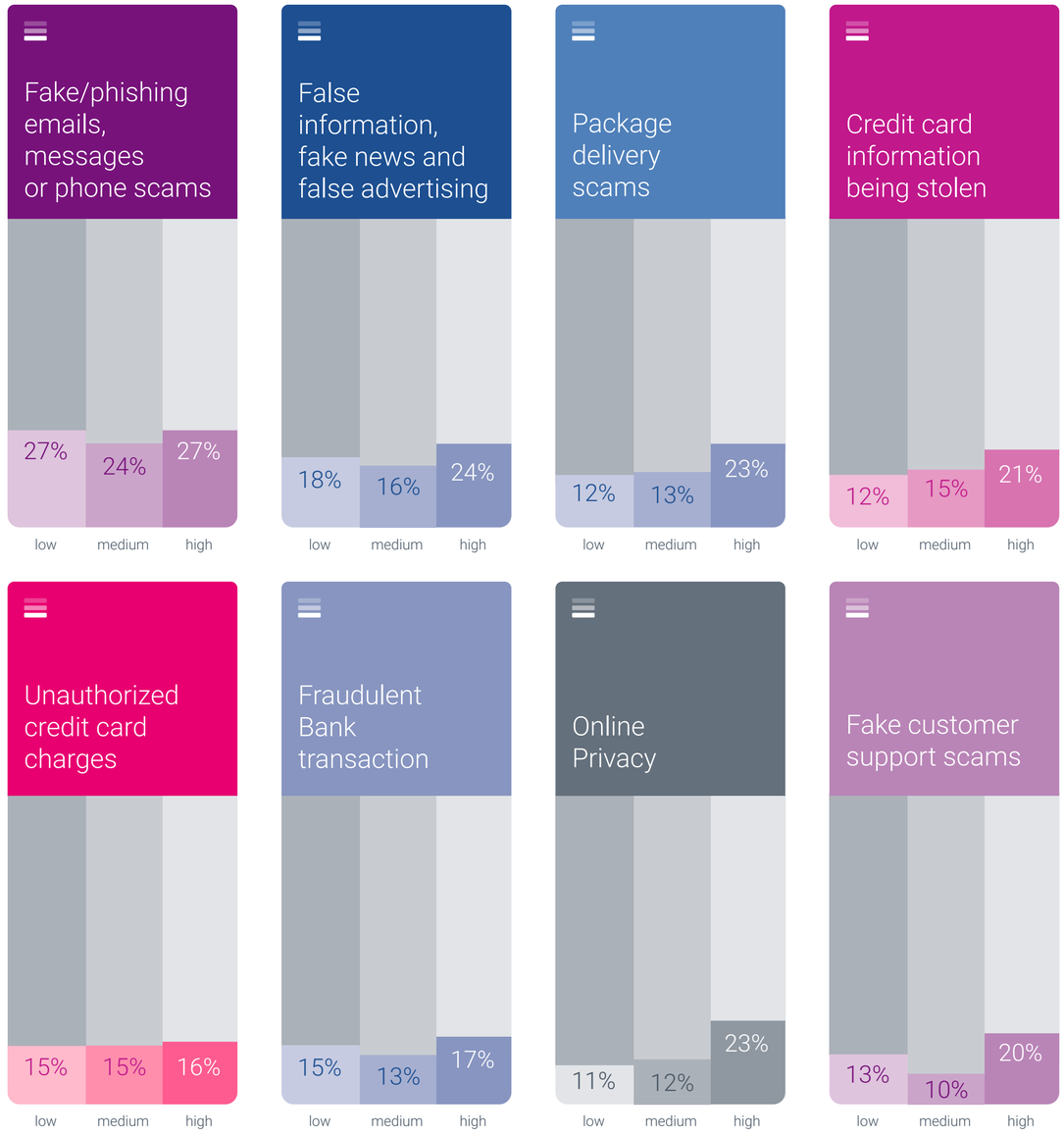
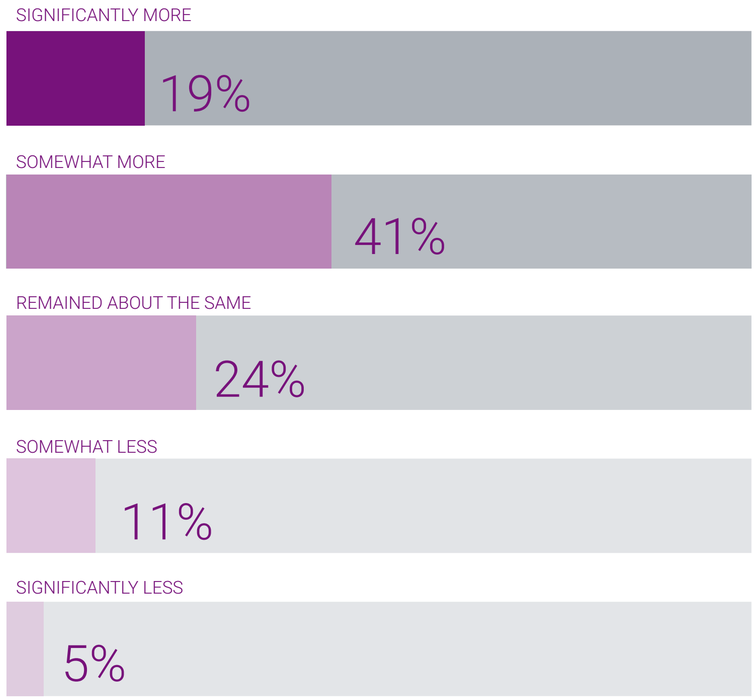


Table 03: Fraud losses changed relative to previous years among businesses



60% of U.S. businesses report fraud losses have increased.

Businesses are seeing the same persistence, with 60% of U.S. businesses saying that fraud losses are somewhat or significantly higher than in previous years. Fraud types such as transactional payment fraud, first-party fraud, identity theft, GenAI-related fraud and money mule scams continue to pressure organizations. Seventy-seven percent of businesses expect to increase their fraud management budgets in 2026, with nearly 80% citing an increase of at least 8%. This is a sign that fraud prevention has become a sustained business priority rather than a temporary response.

This makes fraud more than a loss-prevention issue. It's now a business resilience issue. Organizations must track the direct cost of fraud, but also the effects on customer trust, abandonment, false declines, complaints and brand confidence. Consumers are adding to that pressure. Eighty-six percent expect businesses to respond to fraud and security concerns, which places fraud prevention squarely inside the customer relationship.

WHAT BUSINESS LEADERS CAN DO

The challenge moving forward will be delivering stronger protection without making security feel heavier. Both studies suggest the future of digital trust depends on businesses' ability to make security more intelligent, adaptive and minimally disruptive.

- Benchmark fraud exposure against current market and industry trends.
- As AI-powered scams increase, assess controls across onboarding, login, payments, account changes and customer engagement.
- Track fraud's impact beyond losses, including abandonment, complaints, false declines and customer confidence.

_CHAPTER 02

Fraud is moving from theft to deception

The persistence of fraud is only part of the story; fraud is also changing form. Traditional risks such as stolen payment credentials, unauthorized charges, account takeover and identity theft remain important. But the next wave of fraud adds a different challenge: convincing digital deception at scale.

Fraudsters are increasingly imitating the signals people rely on to decide whether something is real. Emails, text messages, websites, documents, voices, images, customer support interactions and brand communications that appear authentic enough to influence behavior. AI is accelerating this shift, but the broader issue is authenticity. Consumers are already aware of this new environment. Sixty percent have heard of AI-generated fake images or videos being used in scams. Fifty-three percent are aware of AI-generated phishing messages. Forty-seven percent are aware of deepfake voice impersonation. Forty-five percent are aware of AI impersonation of friends or family, and 44% are aware of chatbots impersonating companies or customer support.

Concern is rising with awareness. Nearly half of consumers say they feel more like a target for fraud than they did a year ago, and more than half say they are very or extremely concerned about AI-enabled scams. This changes what consumers expect from businesses.

Not only do they expect companies to respond to fraud and identity-related concerns through stronger online security, clearer communication and more visible protection measures, they also expect responsibility for fraud reimbursement to be shared across the ecosystem, with the greatest responsibility placed on banks and retailers/platforms.

23%

of low-income consumers say they have not heard about AI-related scams.

Table 04: Consumer awareness of AI-enabled scam types by income level

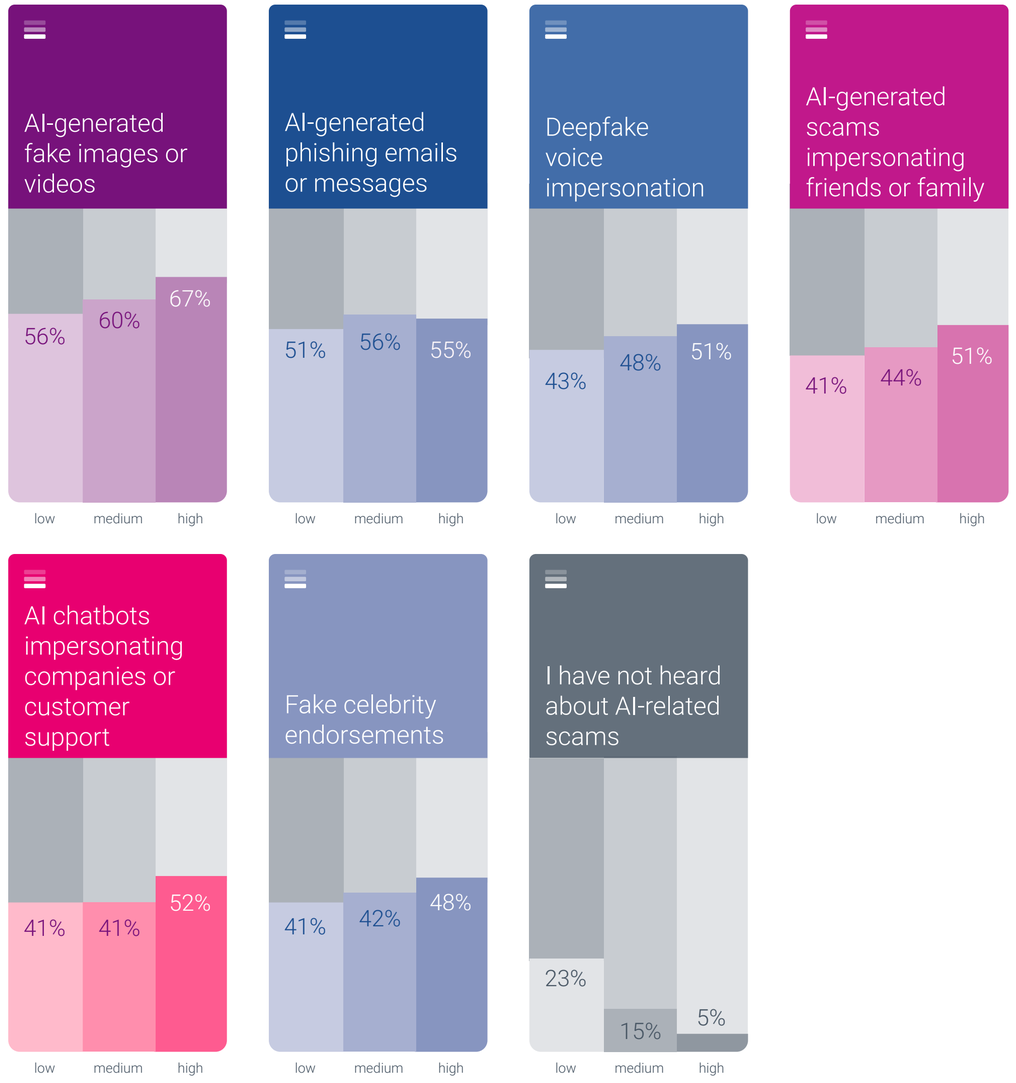
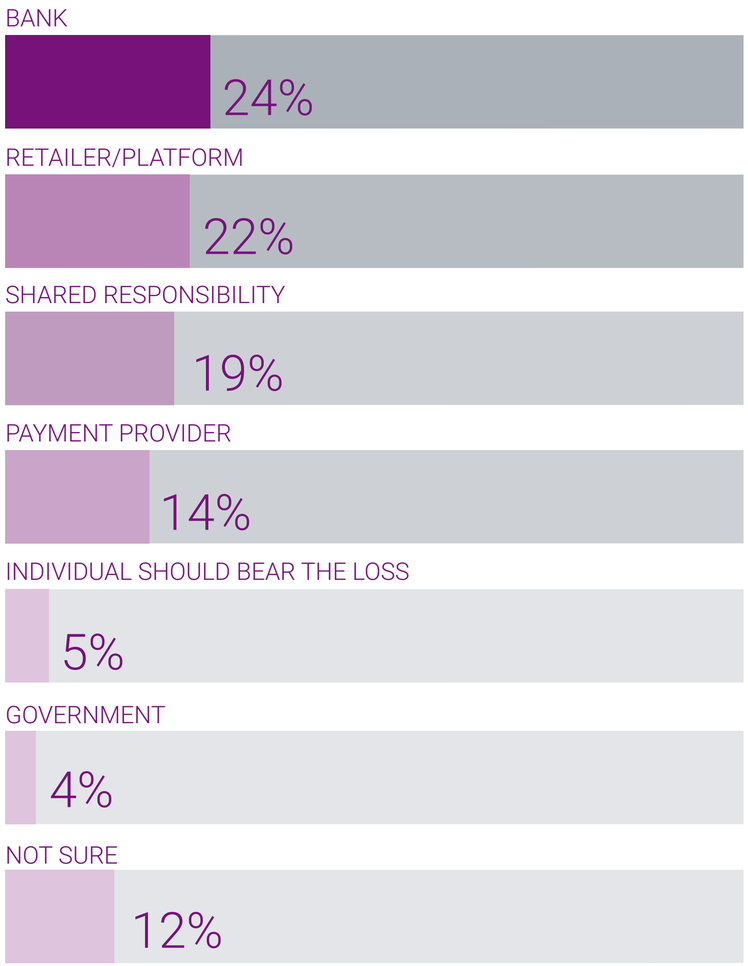


Table 05: Consumer fraud reimbursement responsibility expectations



For businesses, the implication is clear: fraud detection can no longer focus only on the transaction. A suspicious payment, login or account change may be the final step in a longer chain of impersonation or manipulation. Messages, documents, devices, accounts, behaviors and communication channels all become part of the risk picture.

This shift places new demands on fraud teams. Controls designed only to detect transaction anomalies won't be enough. Organizations will need layered intelligence that considers identity, device behavior, document authenticity, communication channels and customer context. As fraud becomes harder to recognize, the ability to establish authenticity becomes more important. That shift places identity at the center of digital trust.

32%

of younger consumers aged 18–24 believe retailers/platforms are accountable for fraud reimbursement, and 27% are open to shared responsibility models.

vs.

22%

of higher-income consumers are more supportive of shared responsibility and 16% are in favor of payment provider accountability.

Table 06: Primary areas of AI-enabled or AI-assisted fraud risk for businesses by industry

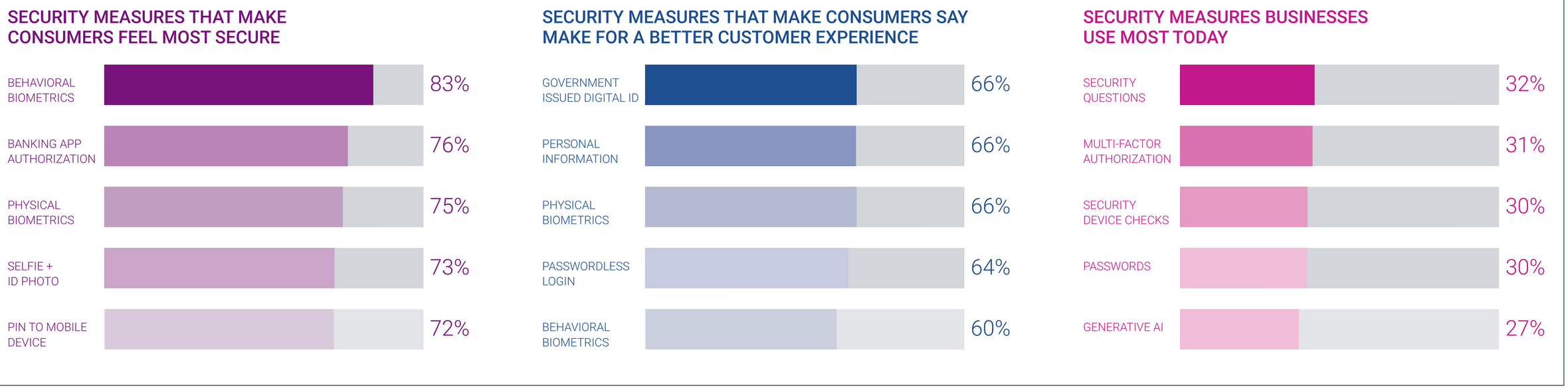
WHAT BUSINESS LEADERS CAN DO

- Evaluate exposure to AI-generated phishing, synthetic identity, deepfakes and document forgery.
- Educate customers on emerging impersonation risks and how to verify authentic communication channels.
- Expand fraud signals beyond transaction anomalies to include authenticity and identity signals.

_CHAPTER 03

Identity becomes the foundation of digital trust

Table 07: Security measures that make consumers feel most secure and solutions businesses are using to detect and protect



As digital interactions become easier to imitate, authenticity can no longer be assumed; it has to be established. That shift puts more weight on identity. It's no longer a simple gatekeeping check at the door; it now underpins fraud prevention, personalization, privacy and the everyday confidence consumers bring to digital experiences.

Consumers increasingly recognize the value of accurate digital identity. Seventy-one percent say it's important for businesses to accurately recognize them online. Nearly half say they become more trusting when businesses recognize them without requiring repeated authentication.

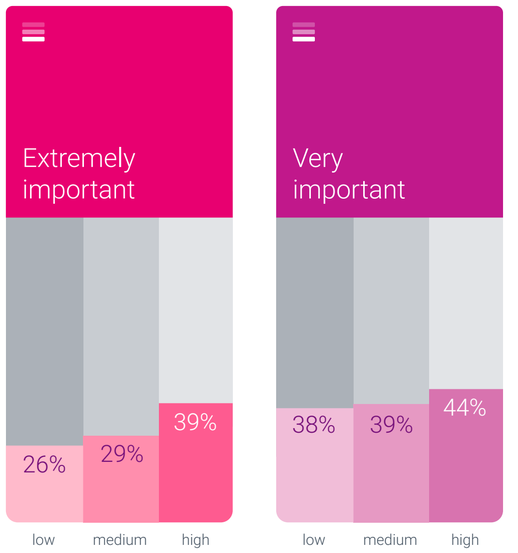
The security methods consumers value most also show how expectations are changing. Behavioral biometrics generate the strongest feelings of security among consumers at 83%. Banking app authentication, physical biometrics, selfie and ID verification, and passwordless login also rank highly.

These methods tend to feel more embedded in the experience, especially when compared with more traditional approaches that can feel repetitive or easy to compromise.

Businesses are still using foundational controls, but the market is moving toward more layered identity strategies. Security questions and multifactor authentication remain among the most widely used fraud prevention solutions. At the same time, organizations are expanding into document verification, physical biometrics, AI-powered document forgery and deepfake detection, machine learning, behavioral analytics, identity graph intelligence, and adaptive risk-based authentication.

The gap between what consumers say makes them feel secure and what businesses most commonly deploy is important. It doesn't necessarily mean businesses are behind. It reflects the pressure organizations face to manage many types of fraud at once while supporting customer experience and preparing for AI-enabled threats. No single control can address every risk or customer scenario.

Table 08: Importance of accurate online recognition by household income



The strongest identity strategies combine multiple signals so organizations can adapt authentication based on risk, context and customer familiarity. A familiar customer completing a routine action should not always face the same controls as an unfamiliar device attempting a sensitive account change. That distinction is where identity intelligence creates value.

New account opening is one of the clearest examples of identity functioning as both a security and experience capability. Consumers expect the process to be fast and intuitive, but they also need confidence that the business is legitimate and that their information is protected. For businesses, onboarding is a high-risk moment because fraud controls must detect synthetic identities, stolen credentials and manipulated documents without creating unnecessary abandonment. The first experience with identity verification can shape whether the customer views the relationship as secure, efficient and worth continuing.

Being recognized is also becoming an expectation of the customer experience. Organizations that can recognize legitimate customers with greater confidence can reduce unnecessary friction and strengthen trust. Organizations that can't may either expose themselves to fraud or burden good customers with excessive controls. Stronger identity verification can improve protection, but consumers will judge those controls by how they experience them.

39%

of higher-income consumers consider accurate recognition extremely important.

vs.

26%

of low-income consumers, highlighting stronger prioritization among higher-income groups.

WHAT BUSINESS LEADERS CAN DO

- Treat identity management as a strategic capability across fraud, customer experience, privacy and trust.
- Evaluate where authentication creates unnecessary friction for legitimate customers.
- Invest in adaptive authentication and identity intelligence that can respond to risk in real time.

_KEY TAKEAWAYS

Consumers increasingly expect account opening experiences to feel immediate and intuitive
Speed, simplicity, and reduced friction are becoming baseline expectations, with consumers showing low tolerance for lengthy or repetitive onboarding processes.

Consumers are willing to complete additional security steps when the purpose feels justified
Across the section, consumers show growing acceptance of verification and authentication measures when they are clearly connected to fraud prevention and account protection.

The onboarding experience increasingly shapes long-term trust perceptions
Consumers appear to evaluate organizations early in the relationship based on how secure, transparent and seamless the account opening process feels.

Consumers increasingly expect businesses to manage security without creating unnecessary burden
There is growing expectation that organizations should proactively detect risk and streamline identity verification in ways that minimize friction while still maintaining strong protection standards.

_CHAPTER 04

The protection-patience paradox

Consumers expect digital experiences that are both secure and efficient. That expectation is now shaping how they evaluate the organizations they choose to trust.
The consumer study shows that people will tolerate additional friction when the purpose is clear. Eighty-four percent say they are willing to complete additional security steps if doing so helps prevent fraud. That finding shouldn't be read as permission to add friction everywhere. It points to a more specific expectation: consumers want security that feels proportionate to the risk.

57%

of high-income consumers are very willing to accept added friction, whereas younger consumers (18-24) show the highest resistance, with 10% saying they are not at all willing to complete additional security steps.

The first minute of a digital interaction has become an important trust window. Consumers have the lowest patience for delays in routine digital interactions, e.g. booking a table at a restaurant or accessing their bank account, reinforcing the expectation that everyday transactions should feel immediate and seamless.

That makes speed a relationship issue. If the experience feels slow, confusing, or needlessly repetitive, customers may interpret the friction as a sign that the organization doesn't know them well enough to serve them effectively and abandon the journey or reconsider the relationship.

The business study reflects the same tension. Companies are under pressure to strengthen controls, modernize authentication, and reduce losses. They also recognize that overly restrictive controls can affect engagement and conversion, and, for repeat customers, erode loyalty and trust. This is the protection-patience paradox: stronger security is essential, but security that feels heavy can weaken the relationship it's meant to protect.

Consumers judge friction by context and are willing to accept added security steps when fraud prevention is clear. A stronger step-up may feel appropriate during account opening, account recovery or a high-value transaction. The same experience may feel unnecessary during routine access from a familiar device. Adaptive authentication helps organizations apply security more intelligently, strengthening controls when risk is higher and reducing unnecessary steps when confidence is already strong.

For businesses, the practical goal is to improve fraud and experience outcomes together. A fraud strategy that reduces losses but increases abandonment may not deliver the intended business outcome. A digital experience that maximizes speed but leaves customers exposed won't sustain trust. The right scorecard should include fraud losses, false declines, abandonment, conversion, complaints and customer satisfaction together.

Table 09: Willingness to complete additional security steps by income

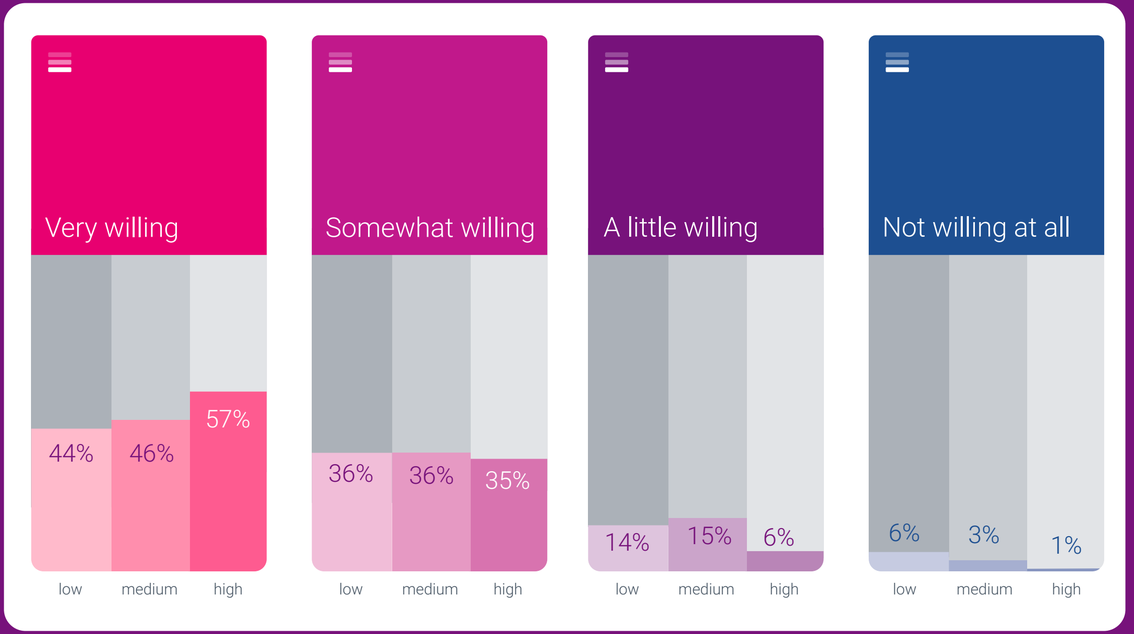
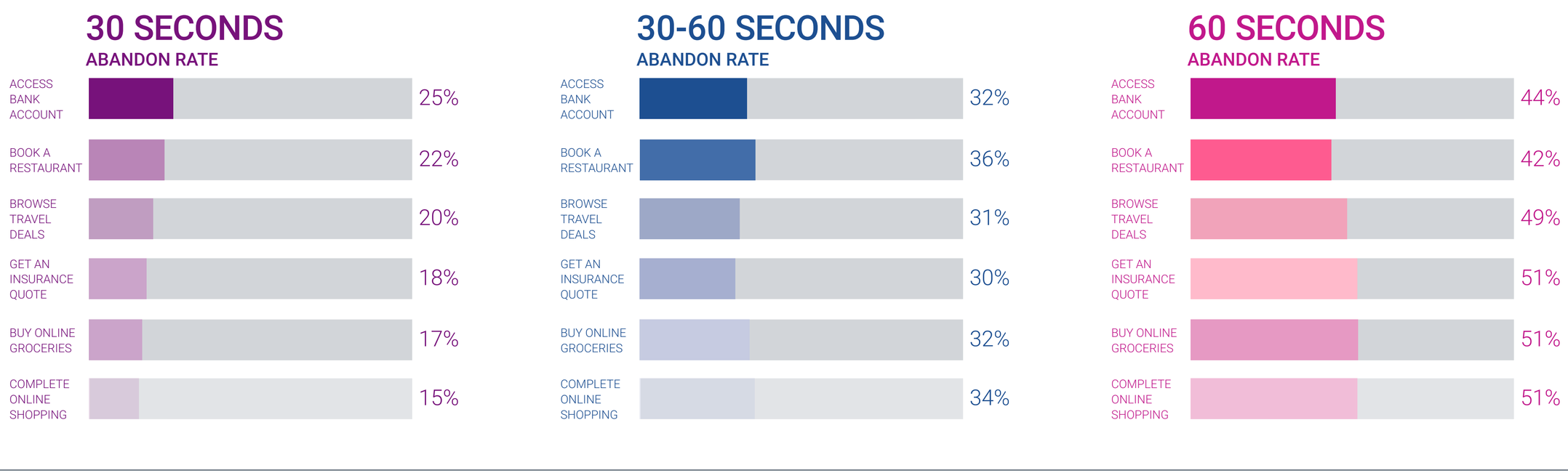


Table 10: Time before consumers abandon selected online activities



Older consumers tend to allow more time before abandoning experiences across several categories, reinforcing that willingness to wait is shaped not only by technology expectations, but also by transaction context and urgency.

WHAT BUSINESS LEADERS CAN DO

The challenge moving forward will be delivering stronger protection without making security feel heavier, both studies suggest the future of digital trust depends on businesses' ability to make security more intelligent, adaptive, and minimally disruptive.

- Map high-friction points in onboarding, login, account recovery and payments.
- Apply adaptive authentication so security intensity reflects the risk of the moment.
- Measure fraud, abandonment, conversion and customer satisfaction together.

_CHAPTER 05

Data control becomes a trust signal

Fraud prevention, identity verification and AI all depend on data. Consumers understand that data powers digital experiences, but they're more selective about what data is collected, how it's used and how it's protected.

The consumer results show a clear control gap. Only 23% of consumers say they feel complete control over how their personal data is used online today. By contrast, 56% say they want complete control. Sixty-four percent want more control over their personal data across at least some online activities.

However, a desire for control does not mean an unwillingness to share data, especially when the value exchange is clear. Fifty-eight percent of consumers see value in sharing their personal data, with security (72%) and privacy (70%) being the strongest motivators for increased willingness to share personal information.

Businesses appear to recognize the same pattern. Security and privacy rank as the most important dimensions shaping online customer experience priorities, at 87% and 81%, respectively. This suggests organizations understand that trust is built not only through ease and personalization, but also through responsible data practices.

As organizations rely more heavily on data to support fraud prevention, identity verification and AI, governance becomes part of the trust equation. Consumers may not see model monitoring, data lineage or access controls directly. They experience the results through more accurate decisions, fewer unnecessary interruptions, faster fraud detection and clearer communication.

WHAT BUSINESS LEADERS CAN DO

- In addition to required privacy statement pages, consider additional ways to communicate transparency, e.g. why data collected improves security or customer experience.
- Prioritize control options in high-trust moments such as banking, credit, payments and account opening.
- Strengthen data governance before scaling AI-enabled fraud and identity programs.

Table 11: Current control versus desired control over personal data

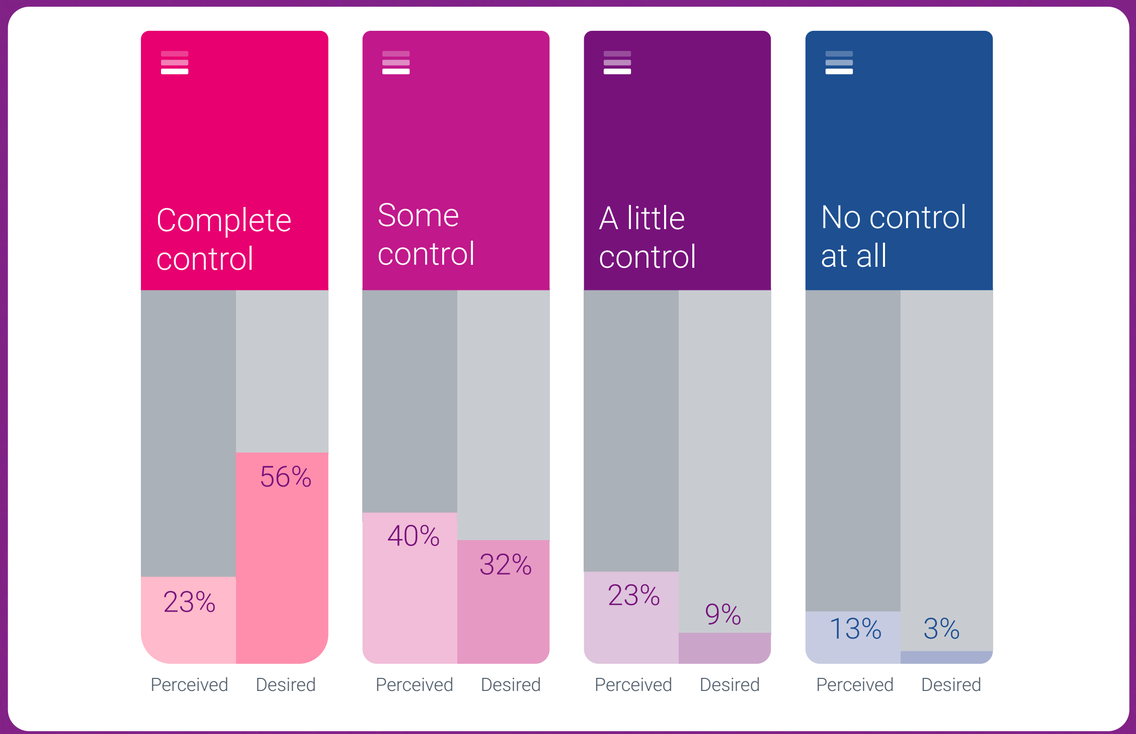


Table 12: Activities where consumers want more control

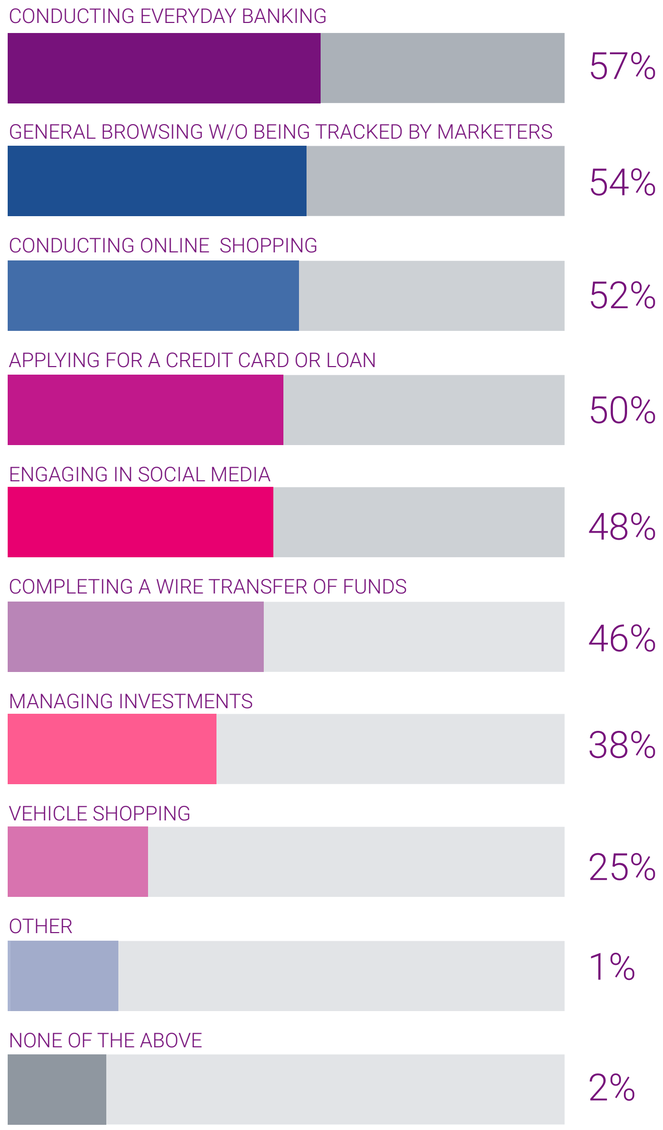
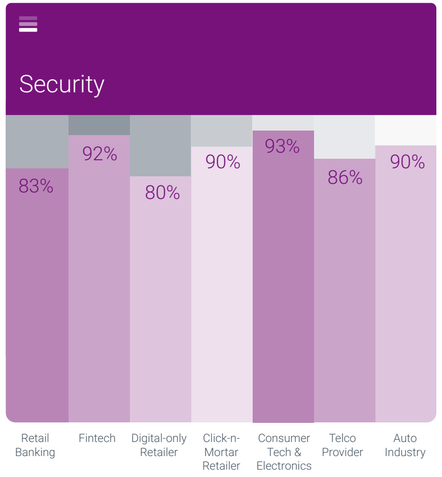
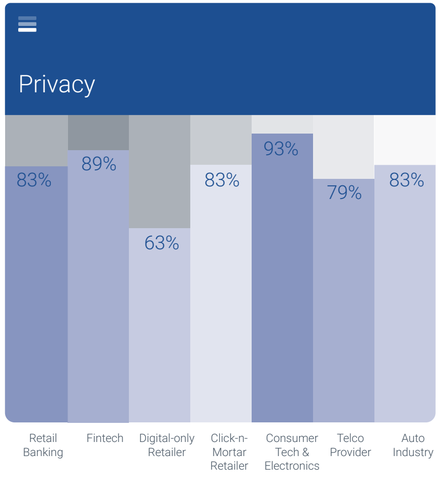
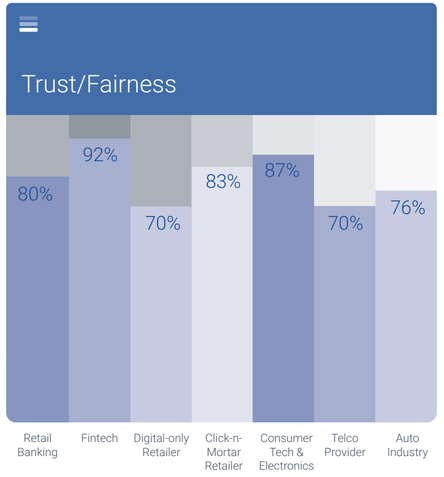
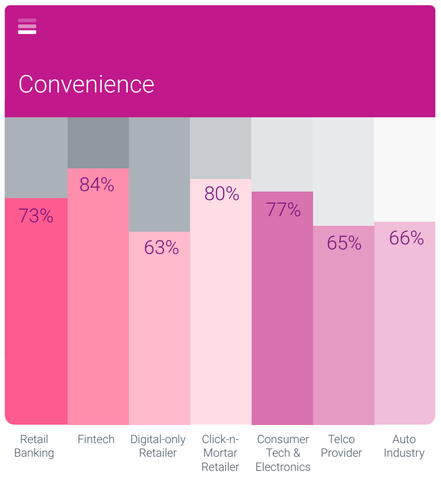


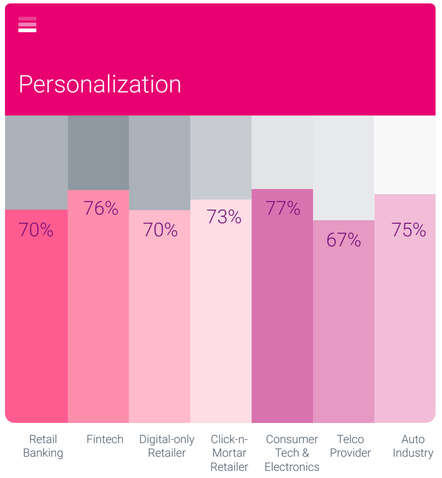
Table 13: Customer experience priorities by industry











_CHAPTER 06

AI changes the fraud equation

AI has been recognized as a fraud threat in our surveys for several years, and awareness continues to grow in this year's results. At the same time, businesses are increasingly using AI to strengthen fraud mitigation and prevention. This dual role—as both risk and defense—makes AI one of the defining issues in fraud and identity.

Consumer adoption is also increasing as people use AI in everyday digital experiences; 27% of consumer-reported account openings were for AI chatbot accounts. This category saw the highest increase in new account openings, up from 16% in 2025. AI can reduce effort, simplify decisions and make digital experiences feel more responsive.

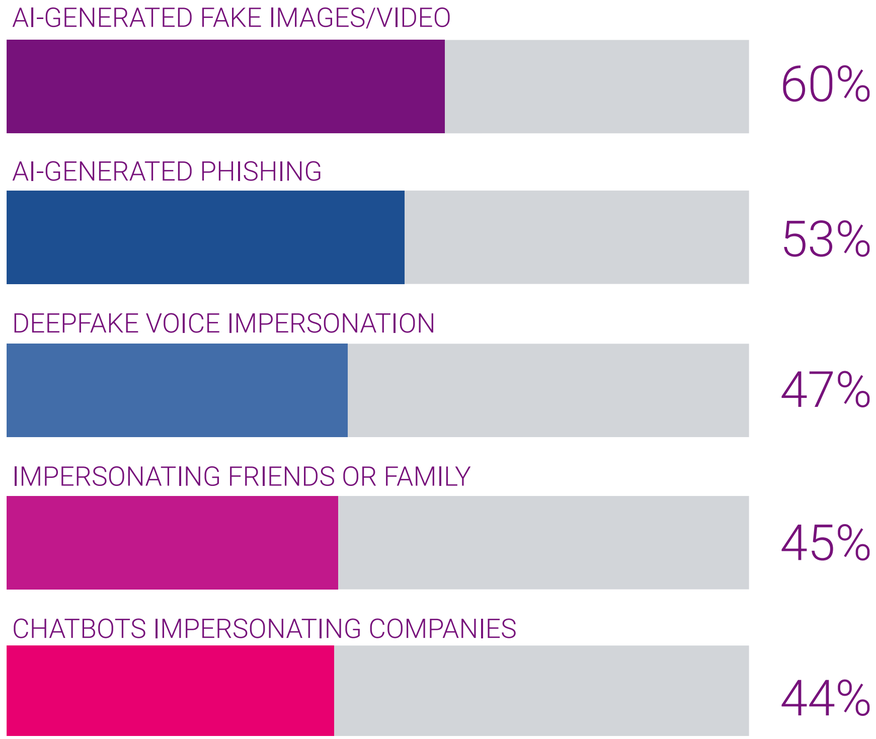
Despite the growing adoption, consumers remain cautious. The same technology that makes digital experiences more useful can also make scams more convincing. This creates an AI trust gap: consumers are willing to use AI when it offers convenience, but they remain concerned about accuracy, transparency and accountability.

Businesses are moving quickly. Eighty percent of U.S. businesses are already using machine learning or generative AI in fraud management environments. AI can analyze large volumes of signals, identify anomalies, detect document manipulation, support adaptive decisioning and reduce manual review burdens.

56%

of consumers are extremely or very concerned about AI scams.

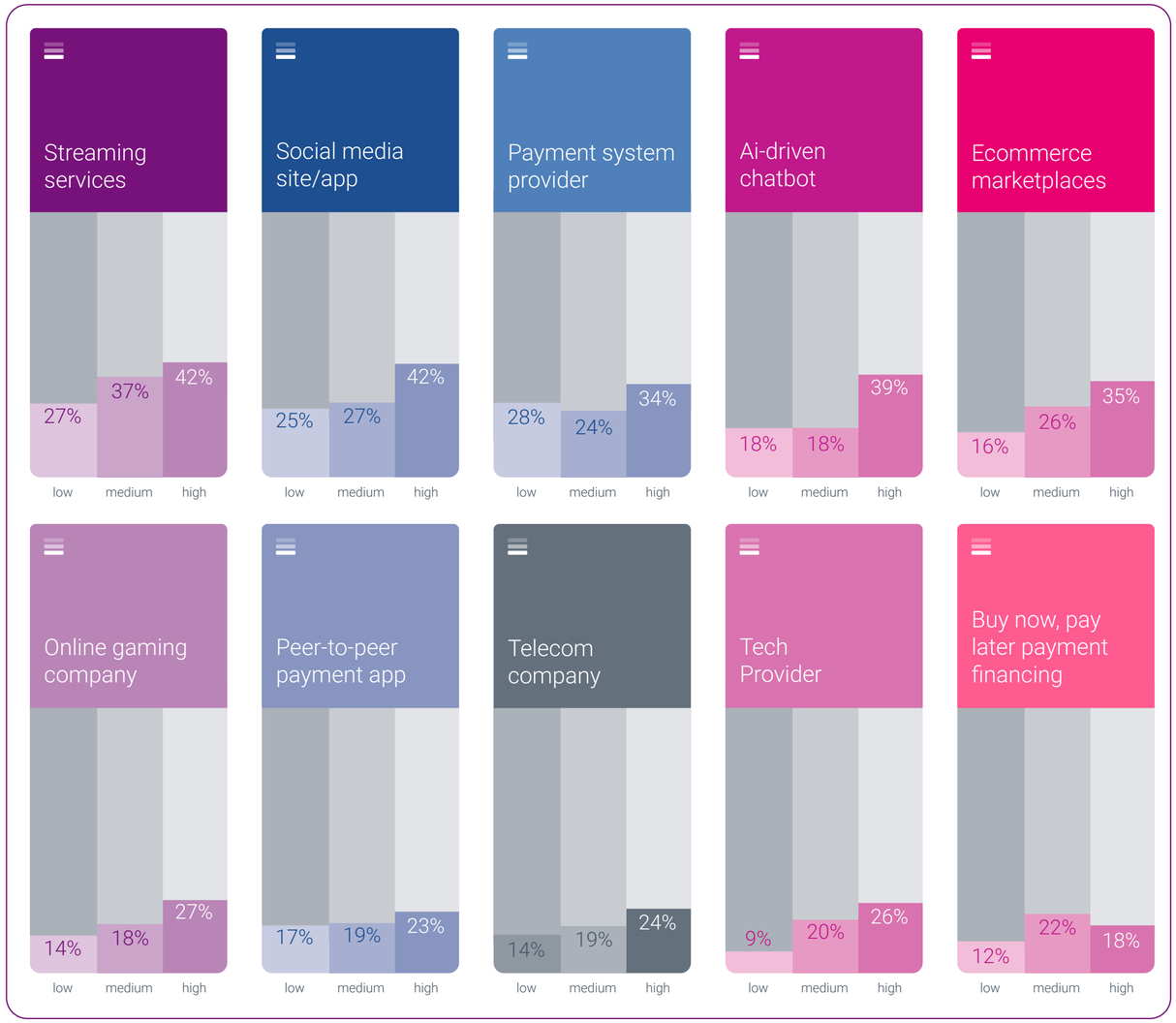
Table 14: Consumer awareness: AI scam types (2025)



27% of new account openings were AI chatbot accounts.

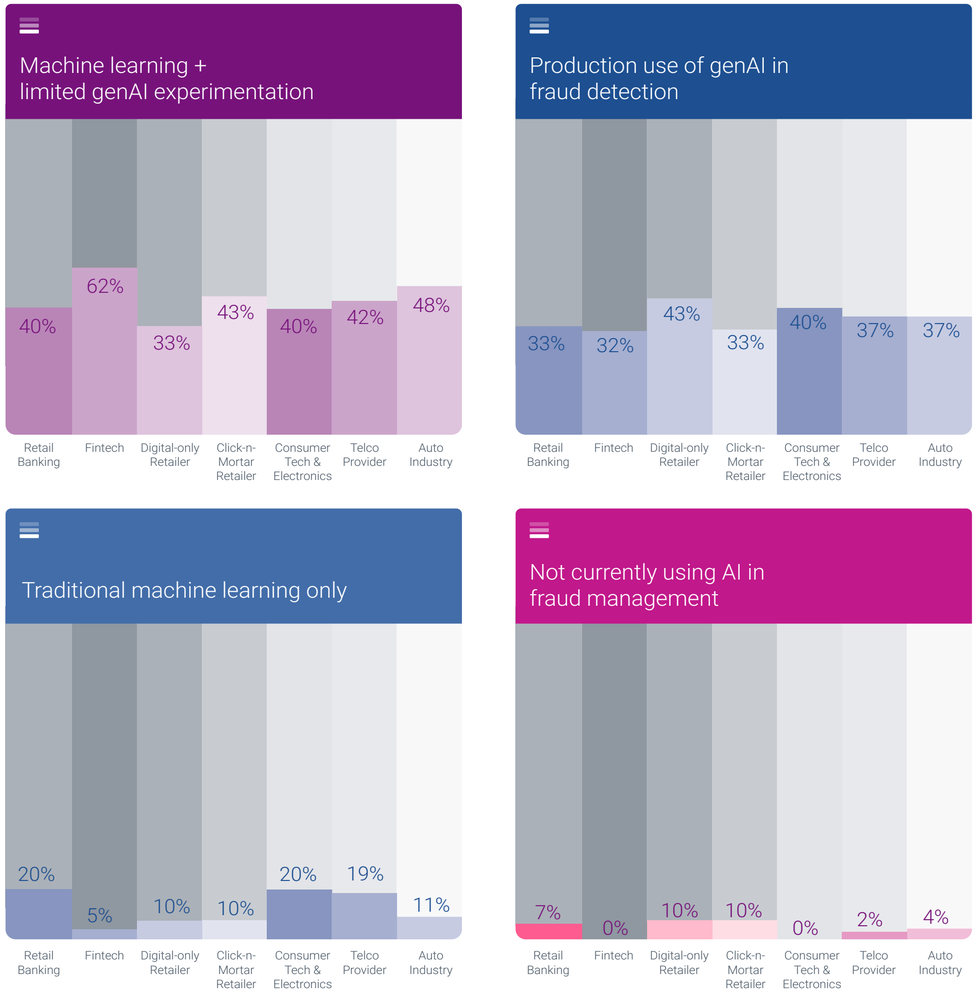
Tables 15 + 16: Types of new accounts opened (Past 6 months)

BY HOUSEHOLD INCOME



BY AGE

Table 17: U.S. businesses adoption of AI in fraud management, by sector



Fraudsters are also keeping pace. Businesses identify AI-generated phishing as the most common AI-enabled fraud risk at 53%. AI-assisted first-party fraud follows at 51%, with AI-generated document forgery at 45%, automated bot attacks at 40%, deepfake voice or audio at 37% and deepfake videos or images at 35%.

As AI becomes more embedded in fraud management, governance becomes essential. Nearly half of U.S. businesses report having formal documented governance and monitoring frameworks for fraud models. Another 29% report informal governance, and 16% say governance is in development.

The next stage of AI in fraud prevention will be defined by disciplined deployment. Organizations will need to strengthen data quality, model governance, identity intelligence and human oversight as AI models and AI agents become more central to fraud management. Those who do this well can use AI to improve both protection and experience.

WHAT BUSINESS LEADERS CAN DO

- Inventory where AI is used in fraud management and customer decisioning.
- Evolve AI governance for fraud models and AI agents, including monitoring and escalation.
- Prepare for AI-generated phishing, document forgery, bots and deepfakes.

_CHAPTER 07

The next horizon: agentic commerce

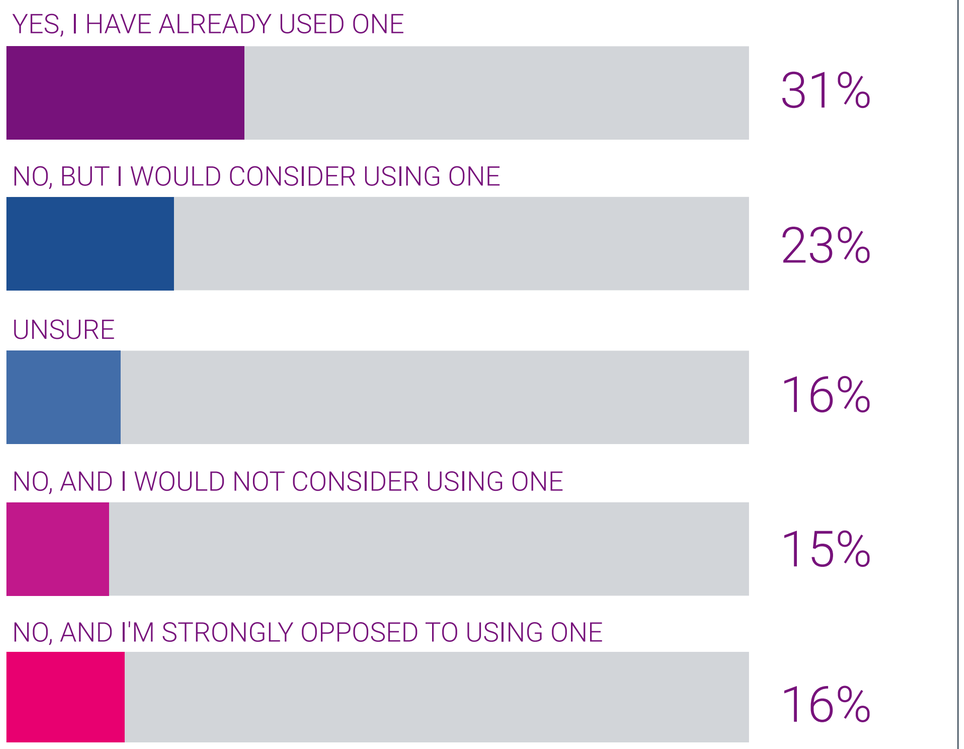
Consumers are increasingly using AI tools to research, compare and support purchasing decisions. AI agents acting on behalf of shoppers will be able to complete purchases autonomously. The consumer data provides an early signal. Thirty-one percent of consumers have already used AI tools to support online purchases or bookings, and 23% would consider doing so. Comfort appears strongest for routine or low-value purchases, however, confidence drops sharply for higher-stakes decisions with just 21% comfortable relying on AI for completing travel-related purchases and only 17% for financial services decisions.

Agentic commerce introduces a human-not-present environment, where consumers delegate certain decisions or actions to AI agents. That shift raises new identity questions. Organizations may need to verify the person, the agent, the relationship between the person and the agent, the permissions granted to the agent, and the context of the requested action.

The business study provides an early bridge to this future. Know Your Agent (KYA) appears as an emerging authentication and fraud-control capability, and businesses using these solutions report high confidence in them. Confidence in KYA solutions reaches 91% among respondents using the capability.

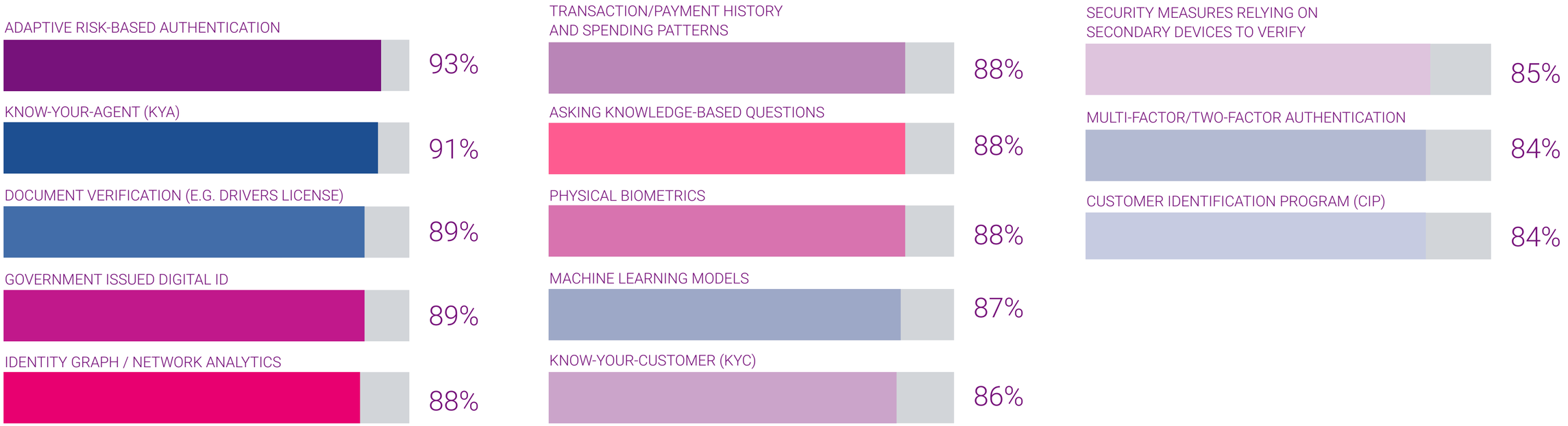
Fraud risks are also evolving. Bad actors will attempt to impersonate legitimate agents, compromise authorized agents, create fraudulent digital actors or exploit weak authorization rules. Businesses will need to begin asking better questions. What permissions would an agent need? How would the organization verify authorization? How will fraud teams distinguish legitimate automation from malicious activity? What happens when something goes wrong, and who is responsible for remediation?

Table 18: AI purchasing adoption and openness



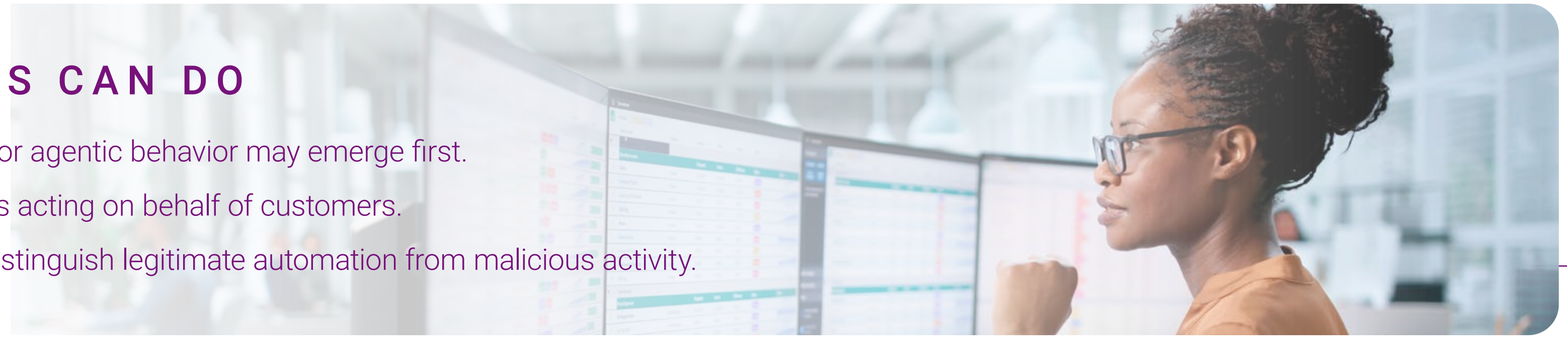
Willingness to engage with AI appears closely tied to broader digital confidence and comfort with emerging technologies.

Table 19: Confidence in Know Your Agent solutions



WHAT BUSINESS LEADERS CAN DO

- Identify customer journeys where AI-assisted or agentic behavior may emerge first.
- Begin defining authorization models for agents acting on behalf of customers.
- Evaluate whether current fraud controls can distinguish legitimate automation from malicious activity.

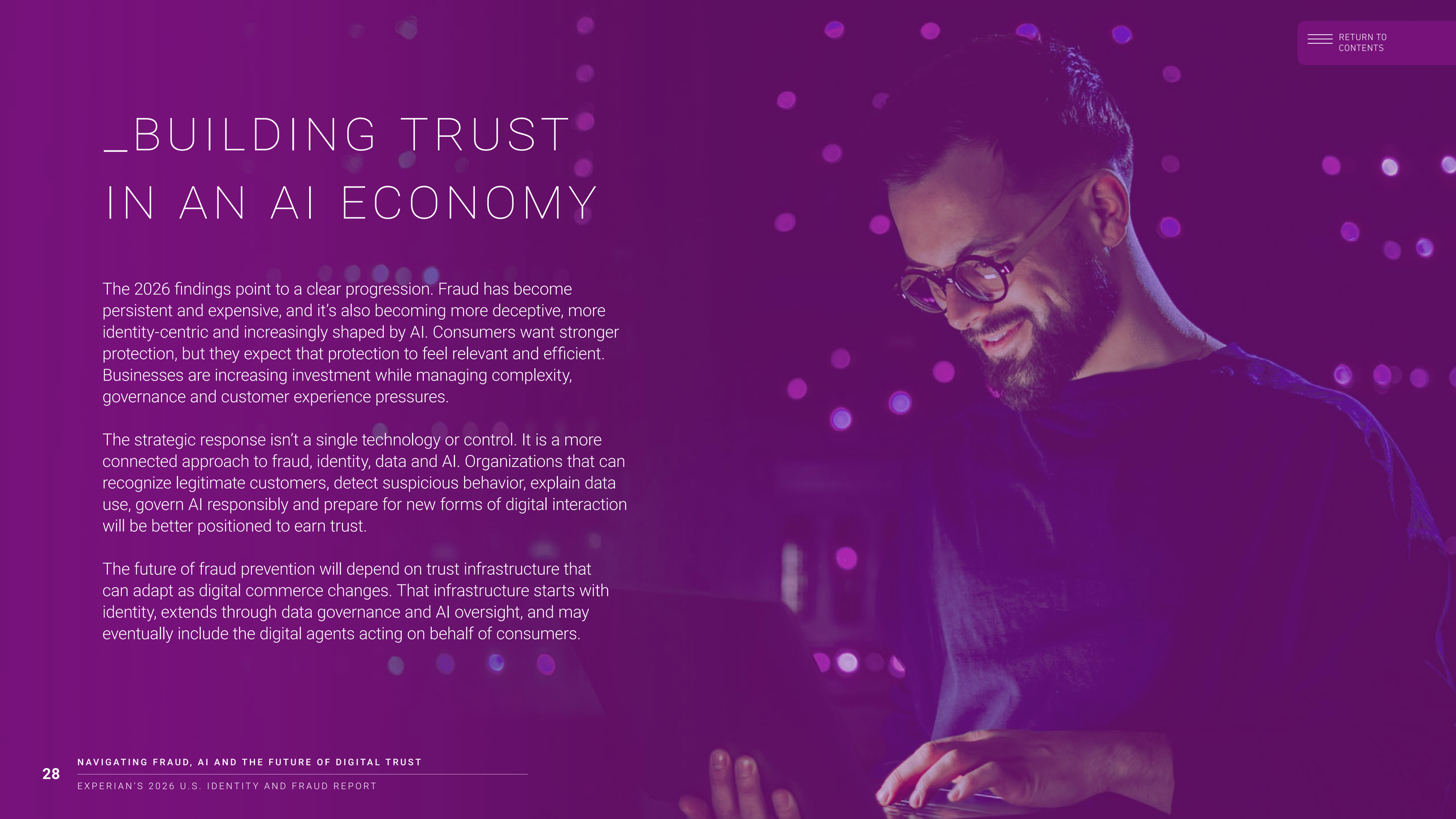


_BUILDING TRUST IN AN AI ECONOMY

The 2026 findings point to a clear progression. Fraud has become persistent and expensive, and it's also becoming more deceptive, more identity-centric and increasingly shaped by AI. Consumers want stronger protection, but they expect that protection to feel relevant and efficient. Businesses are increasing investment while managing complexity, governance and customer experience pressures.

The strategic response isn't a single technology or control. It is a more connected approach to fraud, identity, data and AI. Organizations that can recognize legitimate customers, detect suspicious behavior, explain data use, govern AI responsibly and prepare for new forms of digital interaction will be better positioned to earn trust.

The future of fraud prevention will depend on trust infrastructure that can adapt as digital commerce changes. That infrastructure starts with identity, extends through data governance and AI oversight, and may eventually include the digital agents acting on behalf of consumers.



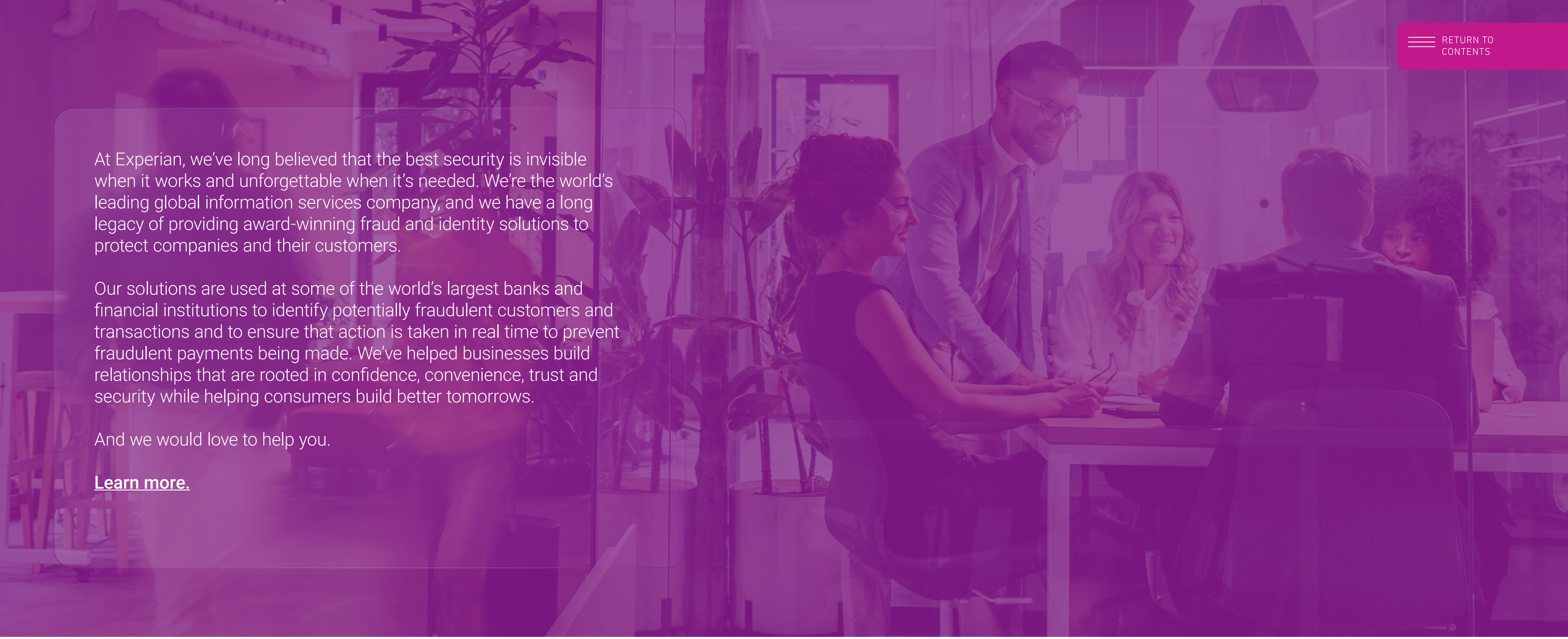
_METHODOLOGY AND SOURCES

The 2026 Experian Identity and Fraud Report marks the 11th year of the study. The report is based on two major surveys conducted in the U.S. in April 2026. 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 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 $1B in revenue. Industries that completed the survey include retail banks, fintech, consumer technology and electronics, payment system providers, and many other companies from a range of verticals.

Public sources referenced in the report:
FTC Consumer Sentinel Network 2025 testimony; FBI 2025 Internet Crime Report.

RETURN TO CONTENTS



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. 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.

Learn more.

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 727 8330
www.experian.com