# Navigating Experience, Security, and the Next Frontier of Identity

Experian's 2024 U.S. Identity & Fraud Report

2024

# _CONTENTS

# _INTRODUCTION

## ABOUT THE RESEARCH

The 2024 Experian Identity and Fraud Report marks the ninth year of the study. The report is based on two major surveys conducted in the U.S. in March of 2024.

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 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.

At the start of last year, many economists were predicting a recession. To their surprise, 2023 clocked an impressive finish, fueled by an increase in consumer and government spending, and increases in manufacturing and private investment.

Following that resilient ending, the U.S. economy entered 2024 facing some familiar headwinds: increased geopolitical turmoil, higher prices, and steady inflation. This brought back an echoing chorus of voices reminiscent of the previous year, asserting that the proverb was true: all good things, in this case growth, must come to an end.

But as we embark on the second half of 2024, the only thing forecasters seem to agree on is that they disagree. While the U.S. is expected to avoid a recession, many economists are citing softening labor market conditions, tighter-than-normal lending standards, and an overall easing in consumer spending and business investment as indicators of slowed growth. Undeterred, bullish analysts on the other side of the spectrum are forecasting continued growth, ranging from 1-3% of GDP.

It’s these same uncertain economic conditions that create an environment ripe with opportunity for fraudsters. Amid an ever-evolving risk landscape fraught with more complex fraud implications, key questions remain for both consumers and businesses:

- How secure do consumers feel online?
- How have their security and experience expectations changed in the last year?
- Are businesses increasing investments sufficiently enough to tackle growing fraud challenges?
- Do they have effective technology solutions in place to accurately identify and authenticate consumers online?
- What impact is GenAI having, or will it have on the fraud landscape in 2024 and beyond?

Experian’s 2024 U.S. Identity and Fraud Report provides answers to these and other questions, providing organizations a clear snapshot of the current fraud landscape, shifting consumer expectations, and insight into how they can prioritize future fraud prevention technology investments.

This year, we also have a first look back at how these trends have changed over the last four years.

# Old methods and new technology drive fraud losses, and keep security a top concern



# _MARKET CONTEXT

It's often said that fraudsters follow opportunity, and the ongoing economic uncertainty and political volatility in 2023 provided a fraud landscape ripe with opportunities. Add to that, technology advancements and new digital tools like GenAI have made it easier than ever before to exploit consumers. All the while, fraudsters continue to leverage fruitful legacy tactics to target the public.

This perfect storm of uncertainty, technology advancement, and opportunity has hit consumers hard, who reported more than $10 billion in fraud losses in 2023, according to the Federal Trade Commission. This staggering number represented a 14% increase over the previous year and the highest dollar amount ever reported.[1] Meanwhile, 60% of credit card holders in the U.S. have been victimized by fraud, with 45% experiencing fraud multiple times. Last year, 52 million Americans had fraudulent charges on their credit or debit cards, with unauthorized purchases exceeding $5 billion.[2]

Coupled with other forms of identity-related fraud like theft and account takeover, U.S. adults lost a total of $43 billion to identity theft and fraud in 2023.[3]

Moreover, many experts believe the number could be even higher because it doesn't take into account losses that went undetected or unreported, due to the shame or stigma of being scammed.

Consumers weren't alone in feeling the impact of fraud. More than 65% of large U.S. financial institutions (assets over $5 billion) experienced increases in the number of fraud attacks and financial crime incidents.[4] Moreover, fraud scams and bank fraud schemes resulted in more than $485B in losses globally.[5]

Beyond consumers and businesses, it gets worse. The nearly half a trillion dollars in fraud joins a flow of illicit dollars from regional and global fraud rings that fund drug trafficking, human trafficking, terrorism, and other criminal activity.[6] "There's a saying in the fraud industry that taking over a checking account or stealing an identity is the 'nicest' thing a fraudster will do that day," said Kathleen Peters, Experian's Chief Innovation Officer for Fraud and Identity. "When we stop or prevent fraud, we are not only protecting consumers and businesses, but preventing a litany of heinous crimes those stolen dollars fund," she said.

[1] https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

[2] https://www.security.org/digital-safety/credit-card-fraud-report

[3] https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html

[4] https://www.pymnts.com/study/state-of-fraud-and-financial-crime-in-the-united-states-aml

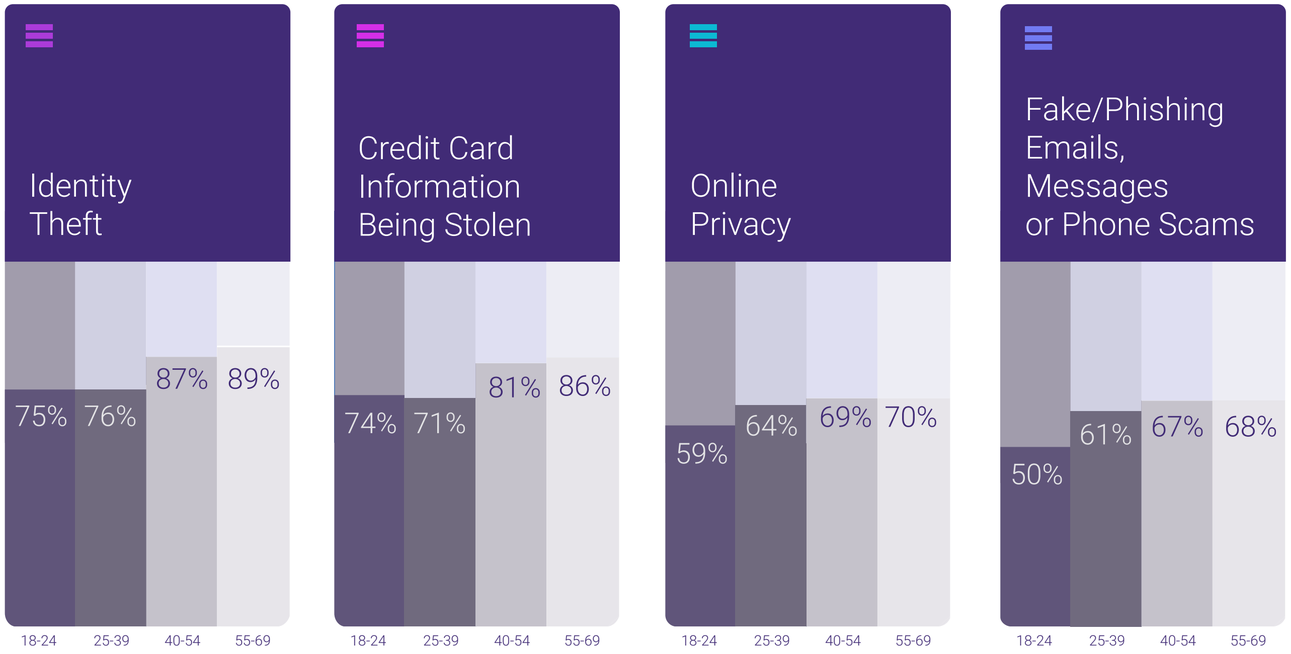
[5] https://bankingjournal.aba.com/2024/01/nasdaq-finds-scams-led-to-486-billion-in-losses-in-2023

[6] https://www.americanbanker.com/news/fraud-cost-500b-illicit-money-topped-3t-in-2023-nasdaq-report

U.S. consumers are incredibly active online, conducting a variety of activities on a daily basis. With this activity comes the awareness that there are risks involved with their digital lives.

As such, this year's research showed most U.S. consumers have a moderate concern about conducting activities online, with 40% saying they're 'somewhat concerned' and 11% reporting that they are 'very concerned' about conducting activities online. While it's still a high number, these numbers are down about ten percent from the previous year, which is surprising considering the increase in fraud losses reported.

**Table 01:** Consumer concerns by fraud type and age category




# Are consumers feeling safer online? The results are mixed.

Similarly, respondents' feeling of being a target online also decreased, with 39% saying they felt like they were more of a target online than they were a year ago, which is a 13% drop from last year's report.

One could interpret the decrease in consumers' concern for conducting online activities and their feeling of being targeted online as a signal that consumers are feeling safer online. It's more likely that consumers have just resigned themselves to the inevitability or ubiquity of fraud, as they remain concerned about specific online security threats.

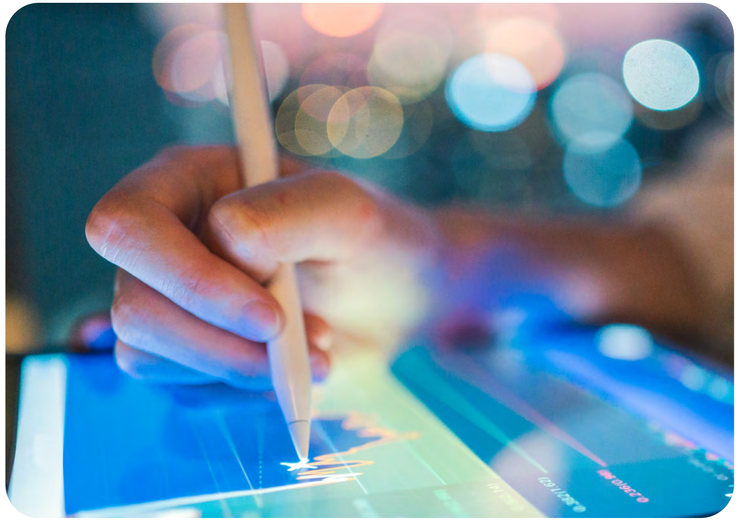
Consumers ranked identity theft (84%) and stolen credit card information (80%) as their top online security concerns, a sizeable jump (+20%) from the previous year for both types. In fact, these two fraud concerns have remained consistently at top of mind for consumers for the last four years.

Notably, younger consumers (those under the age of 39), generally show less concern towards these two areas: identity theft (75%) and stolen credit card information (74%). Additionally, for 2024, online privacy (67%), phishing emails or phone scams (65%), and false information or fake news and ads (49%) round out the top five online security concerns for U.S. consumers.

U.S. businesses are unwavering in their concern about fraud, with more than half of businesses saying they discuss fraud management often, and 28% of businesses indicating that fraud is always discussed. It's not a surprise, then, that nearly half of businesses (46%) report a medium level of concern about the risk of fraud towards their organizations and 41% saying they have a high level of concern. It's important to note, that though they represented a small portion of survey respondents, retail banks showed directionally higher concern (61%) about the risk of fraud in their institutions.

Concern and conversation seem to be translating to a better understanding of the impact of fraud. In this year's survey, 59% of businesses said they 'completely understand' the impact of fraud on their business. Digital-only retailers and retail banks claimed a directionally stronger grasp on the impact of fraud in their verticals at 70% and 65% respectively, reporting a 'complete' understanding.

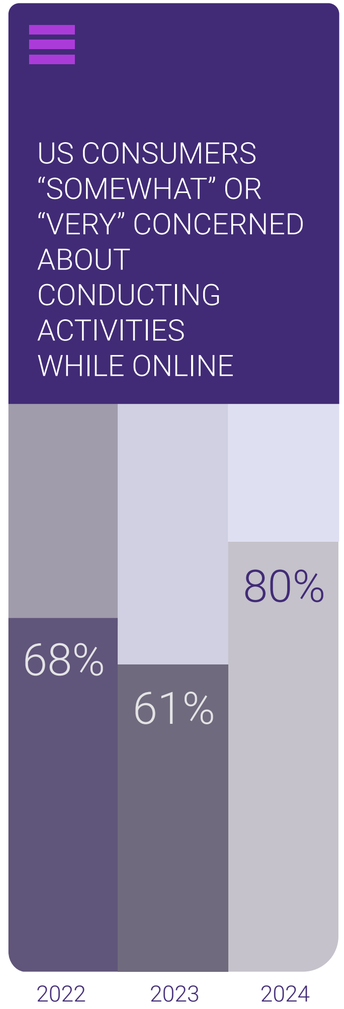
## More concern, more confidence but more fraud for U.S. businesses



Better understanding or not, commercial fraud losses continue to increase. Over 50% of businesses surveyed said that their losses due to fraud had either increased significantly more (24%) or somewhat more (35%) compared to previous years. Interestingly, Fintech and Click-n-mortar retailers reported the greatest decrease in fraud losses (+5 pts) compared to other sectors.

And all this is leading to increased stress for U.S. businesses. Cybercrime was cited as the operational challenge putting the most stress on their business by 45% of companies in this year's survey. Generative AI (GenAI) fraud and/or deep fakes (41%), P2P payment scams (40%) identity theft (39%) and transaction fraud (38%) round out the top five stressors. Notably, looking across companies of different size, Tier 1 businesses listed GenAI fraud (49%) as their biggest stressor. Meanwhile, retail banks cited synthetic identity fraud as the operational challenge putting the most stress on their business.

**Table 02:** A look at online safety and security over the years [ 2022 - 2024 ]



Overall in 2023, Account Takeover Fraud (32%), Identity theft (31%) and Fraudulent New Account Openings (31%) were the most experienced fraudulent events. However, in looking at the first part of 2024, a bit of jockeying has occurred, with Identity Theft (28%), APP Fraud (26%), and New Account Opening Fraud (26%) being the most experienced events.

Businesses are most confident in their ability to protect against First Party Fraud (92%) and Transactional Payment Fraud (90%). At the other end of the spectrum, Cybercrime (75%) and GenAI Fraud and Deep Fakes (70%) are the top expected challenges that businesses think they will encounter in the next 2-3 years.

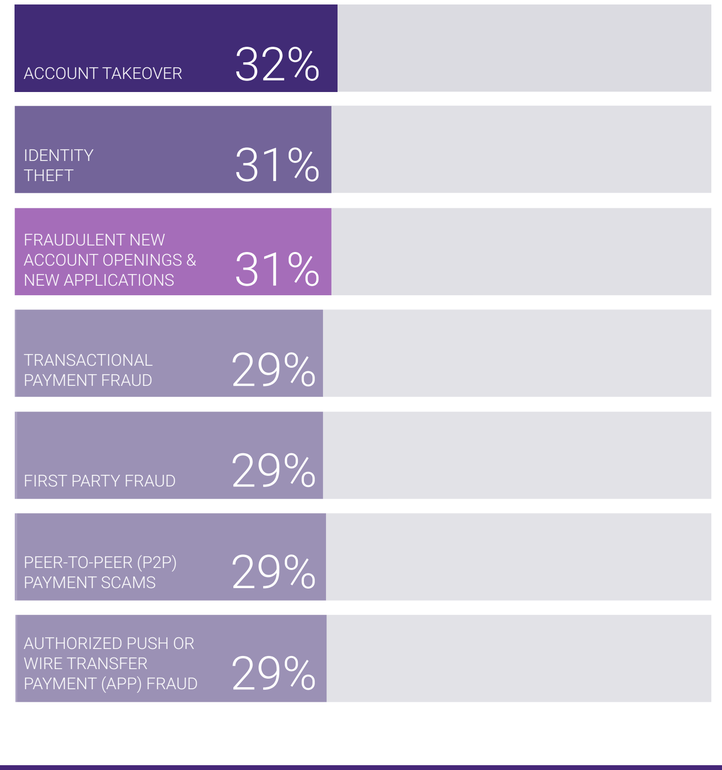
When looking at potential areas of investment to combat fraudulent events, businesses are primarily engaged in improving and building new AI models that address non-customer decisions (60%) and in preventing APP fraud (60%). These areas are expected to receive greater investment throughout 2024.

## _EXPERIAN PERSPECTIVE

Consumers and businesses alike continue to be aligned in their concerns about fraud. Though they may feel a bit safer online, consumers have consistent concerns with specific fraud types. And with their increasingly digital lives, comes new fraud risks from tried-and-true methods and advancing technologies like generative AI (GenAI). As such, continued investment in solutions to combat fraud will be important. However, focusing on one type of fraud will leave businesses and their customers exposed in other areas. And companies won't be able to afford the game of fraud whac-a-mole.

To keep pace with the market, businesses will need to apply a multi-faceted strategy that leverages the right data and tools in an orchestrated way that brings to bear multiple types of recognition and security to stop all types of fraud, while allowing genuine customers through their buying journey.

Table 03: Top most encountered fraud events reported by U.S. businesses



RETURN TO CONTENTS

# Consumers and businesses align on security and experience but not so much on trust

# _MARKET CONTEXT

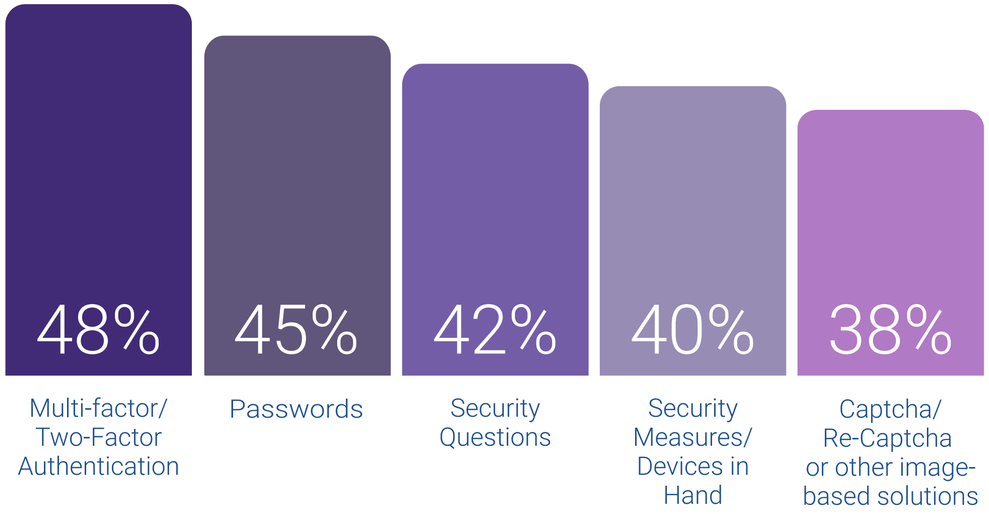
The global pandemic ushered in an era of unprecedented change and digital transformation not seen before. Consumers embraced this shift and it redefined how they approach most, if not all of their social and business interactions. A majority of consumers (88%) indicated that email was the online activity they engaged in the most, followed closely by general media (YouTube, Google, etc.) in second place at 82%. And it's their engagement with these tech giants that is helping to drive consumers' expectations for their online and even real-life experiences. No longer are they bound by brick-and-mortar business hours, geography or device. They can now effortlessly jump from digital channel to app, online to offline.

And with all this ease comes more expectation—the desire for more convenience, and increased accessibility, without giving up security. As such, consumer expectation that businesses will react to their fraud concerns has remained high (above 80%) over the years, clocking in at 82% this year.

Consumers also remain unchanged on the kinds of technologies they feel are secure and create a positive user experience.  And businesses feel like they have it right. More than three-quarters of companies in our survey were extremely or very confident that the security measures they intend to invest in are what their customers want. And the data seems to support that assertion, which is a significant change from last year's report.

Several of the methods consumers find most secure and deliver a better experience are also those methods currently used by businesses today. Businesses cited multi-factor authentication (48%) and the use of Passwords (45%) as the most used fraud prevention methods, followed by security questions (42%), measures that require a customer to have a device in-hand, i.e. one-time passcodes (40%) and Captcha or other image-based solutions (38%).

**Table 04:** Top 5 measures currently used by business for detecting and protecting against fraud




## Consumers are active online, but opening fewer accounts

**Table 05:** Top 5 measures that make consumers feel most secure

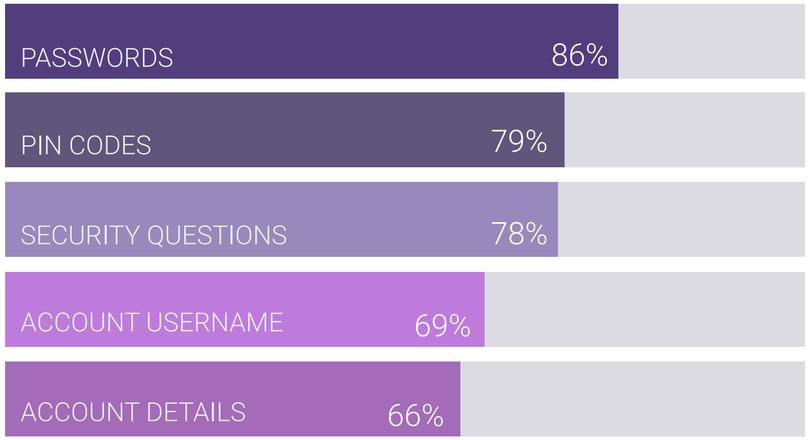
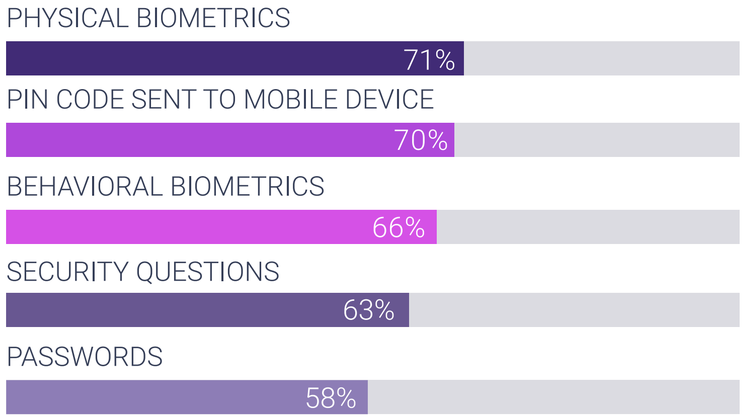



**Table 06:** Top measures that consumers say are important to a better online experience




Increased concern about online security doesn't seem to be dampening consumers' online activity. Not only are consumers going online for email and general media use, but they're also opening new accounts and transacting business. While high-income households showed they were less likely to use general media than other income brackets, instead they're going online to conduct activities such as paying bills, making online purchases, and conducting personal banking. Interestingly, across all income levels, consumers who are 25-39 and 40-54 were directionally more likely to go online for financial activities like applying for a car or home loan.

But here's where it gets interesting. Even with consistent online activity, we observed a decrease in the number of new accounts opened in the last six months. This year, 41% of consumers reported having opened a new account in the past six months, which is down 14%, from 55%, in last year's report.

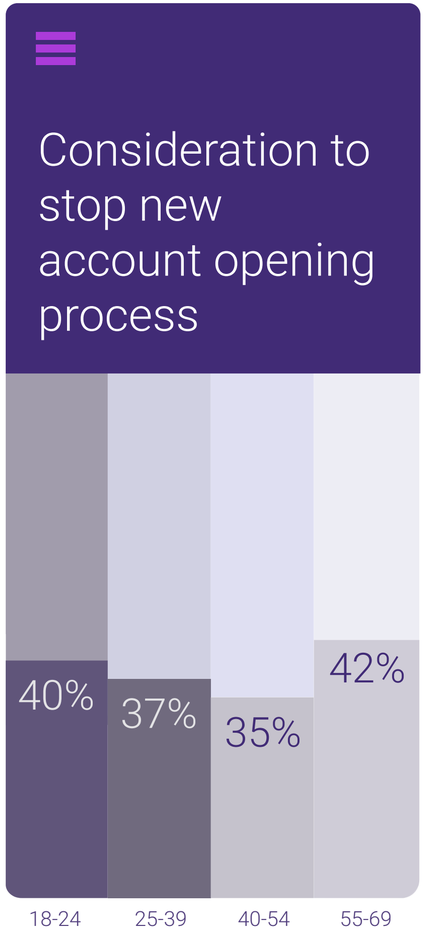
However, of those consumers who opened a new online account, 63% reported having opened 2 or more accounts. Over half (56%) started accounts with organizations that they had no previous interactions with. Interestingly, high-income households (48%) and consumers aged 25-39 (47%) were more likely to have opened an account, whereas consumers aged 55-69 opened the least (33%). Streaming services (36%) and Payment system providers (26%) were the most opened accounts, with Peer-to-peer (P2P) payment apps (24%), social media apps (24%), and retail banks (17%) rounding out the top five.

It appears from this year's research that the account opening process has become more seamless. This year, only 38% of consumers considered stopping a new account opening due to friction in the process, down from 51% in last year's report. Likewise, only 18% of consumers reported actually moving their business to another organization, stemming from their account opening experience. This was an improvement from last year's report, where 37% of consumers reported moving their business elsewhere.

In a further showing of the importance of a positive account opening experience, 66% of consumers reported remaining with the same business because of their positive experience in the account opening process.

## Customer experience and retention improving

**Table 07:** Breakdown of consumers by age, who have moved their business elsewhere due to a negative experience




# Better experience & consistent identity confirmation can lead to increased trust, but are they?

Consumers are recognizing the connection between identity and a positive customer experience, and businesses seem to be responding in kind. In fact, 63% of consumers surveyed expressed it was extremely or very important for businesses to be able to recognize them online.

This ability to repeatedly identify consumers can translate to trust. One-third (33%) of consumers indicated they are extremely or very trusting of businesses that can accomplish easy and accurate identification. Moreover, 48% said they are more trusting of businesses when they demonstrate signs of security.

Financial services companies seemed to be the biggest beneficiaries of this trust, with retail banks, P2P Lending and Buy Now Pay Later financing listed as the top trusted organizations by U.S. consumers, each at 23%. P2P payment apps and payment system providers round out the top five at 20% each.

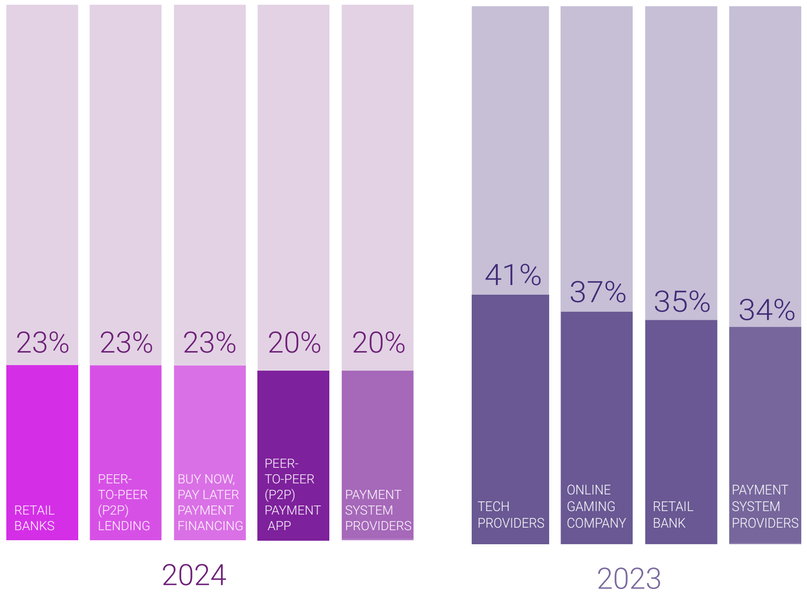
But this isn't necessarily good news, as we observed an overall decrease in consumer trust across industries in this year's data, with trust numbers dropping 10-20% for all industries. Notably, the leaders from last year's report: tech providers and online gaming companies, each dropped more than 20%, landing themselves out of the top five most trusted industries.

# Decreased trust = less willingness to share data

Perhaps it's not surprising when you consider the overall drop in consumer trust, but interestingly, this year we observed a significant decline in consumers who indicated they were 'very willing' to share their personal data. In 2022, 25% of US consumers said they were 'very willing' to share their personal data with businesses online; this number rose to 34% in 2023, however, decreased to 9% in this year's data.

Overall, consumers showing any willingness to share data stayed consistent at around 80%, but the decrease in willingness and decreased consumer trust are signaling shifts in the market that businesses should be mindful of.

**Table 08:** Breakdown of the most trusted businesses by segment



# _EXPERIAN PERSPECTIVE

Clearly, consumers have high expectations for a secure and seamless experience with the companies they engage with. But this year's data showed some seemingly contradictory results. Consumers say they trust businesses that show signs of security, and businesses that can repeatedly and accurately identify them. Most of the security measures that make consumers feel safe and create a positive consumer experience are the ones currently being used by companies. Moreover, businesses are confident that the security measures they intend to invest in, in the future, are the ones consumers want. Meanwhile, new account openings are down, in addition to consumer trust. This year's data showed some seemingly contradictory results, but should it come as a surprise? Consumers are a fickle bunch and while this is frustrating for businesses, it's nothing new.

Perhaps when we look at what's happening in the U.S. and on the world stage, this year's results are even less surprising. The decrease in consumer trust in our survey is consistent with similar results in other industry research, such as Gallup's recent confidence index.[7] Additionally, Qualtrics recently found[8] that consumer trust had dropped to its lowest level since 2016, on par with trust levels from 2012. As trust levels have gone down, concerns about online security, data and privacy have increased. This has only been exacerbated by the emergence of GenAI. Though they've dipped a bit, interest rates remain high due to stubborn inflation levels. In turn, financial institutions have tightened lending criteria and demand for capital has gone down.

The dots are not hard to connect, once you look at the bigger picture. But what are businesses supposed to do in response? Let's start with what we do know: while account opening numbers may have dipped this year, they're still notably high and directionally significant. Moreover, a significant number of individuals who opened new accounts reported opening additional accounts. And a notable number of consumers reported staying with an entity due to a positive account opening experience. Altogether, this means that there are still consumers shopping for credit and services, and they respond to positive experiences with more commerce.

At the intersection of security, accessibility, and convenience is identity. Being able to quickly and accurately confirm consumers are who they say they are, is paramount to a secure, personalized experience. What this year's data does show is that companies will need to double down on their ability to easily, accurately, and repeatedly confirm consumer identities. This is not only for security, fraud prevention and trust, it could also impact consumers' willingness to share data in the future. This in turn could impact businesses' ability to continue to provide a secure, personalized experience.

The adage is still true, you only get one chance to make a first impression. First impressions are strong influencers on trust and set the tone and the course of the future customer relationship. But getting that first experience right is just the first step. Consumers want to know businesses are protecting them and that their expectations are being met. Businesses should consider reminding consumers what they're doing to protect them. This shouldn't come in the form of additional friction, however, but signposting the security measures they have in place to protect consumers throughout their customer journey.

Beyond increased consumer engagement, businesses will need to look at tools like behavioral analytics and other fraud prevention technologies that examine behavior patterns to quickly disarm bot attacks, or coordinated fraud attacks. These coupled with systems that allow for accurate and repeatable identity confirmation and verification, will ensure businesses not only establish trust with consumers but can keep and grow that trust.

[7] https://news.gallup.com/poll/1597/confidence-institutions.aspx

[8] https://www.xminstitute.com/blog/12-years-trust-ratings

# The meteoric rise of GenAI and the resulting implications

# _MARKET CONTEXT

Generative AI (GenAI) is a subset of artificial intelligence techniques that involve algorithms capable of creating realistic content, such as text, music, images, code, etc. from input data. These systems, like Chat GPT, DALL-E, and others use machine-learning models, especially deep learning, that are trained on vast data sets that work in a self-supervised way to identify patterns for a wide range of tasks, generating outputs that mimic human-created content.

If its pervasiveness in the cultural zeitgeist isn't enough of an indication, GenAI is more than just the latest tech trend. What started as the most hyped tech story of 2023, quickly turned into some of the biggest business news of 2024. Companies like NVIDIA saw their stock soar due to increased and anticipated demand for chips to train and run AI models and programs.

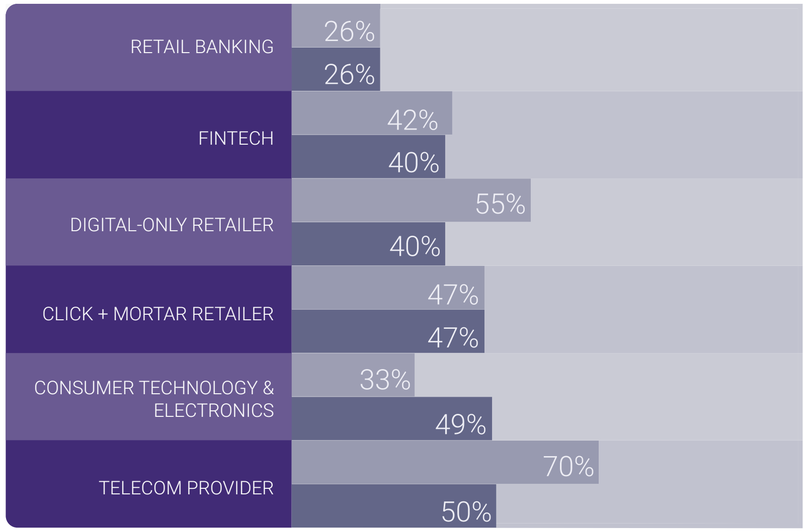
From the typewriter to the computer, previous technological breakthroughs have transformed the way people work. These along with a litany of other innovations were touted for improved efficiency and increased worker output. It's these same characteristics, along with a litany of others including upskilling workers, data mining, improving customer experience, etc. that are driving business adoption of GenAI.

Verizon is successfully using GenAI to improve customer satisfaction and loyalty.[9] Expedia and Wayfair are leveraging it in the form of AI assistants so customers can better leverage their travel and home décor services, respectively.[10] Meanwhile, tech companies like Microsoft and Adobe have already embedded GenAI capabilities into their platforms and products that their customers use every day. The possibilities are seemingly endless, as is the impact. Some strategists are saying the boom could deliver $650B to US GDP in the next decade; globally the impact could be even more substantial at 1.2T – 2.4T.[11]

Unsurprisingly, companies in our 2024 survey also see the benefit of GenAI in their businesses. Overall, they reported high engagement and investment in Gen AI, as well as AI models that improve customer decisions, and Gen AI security solutions.

While businesses seemed bullish on the utility of GenAI to create efficiencies and improve customer experiences, they do see the potential negative impacts it can have. In this year's survey, GenAI fraud and deep fakes came in second on the list of top operational challenges putting stress on businesses. It was preceded only by Cybercrime, at 45%, an area of fraud that is increasingly employing GenAI to perpetrate crimes. Interestingly, Tier 1 businesses listed GenAI fraud as their top stress point.

**Table 09:** Breakdown of Stress Percentages for Cybercrime & GenAI Fraud across industries





[9] https://www.reuters.com/technology/artificial-intelligence/verizon-uses-genai-improve-customer-loyalty-2024-06-18

[10] https://www.wsj.com/articles/how-did-companies-use-generative-ai-in-2023-heres-a-look-at-five-early-adopters-6e09c6b3

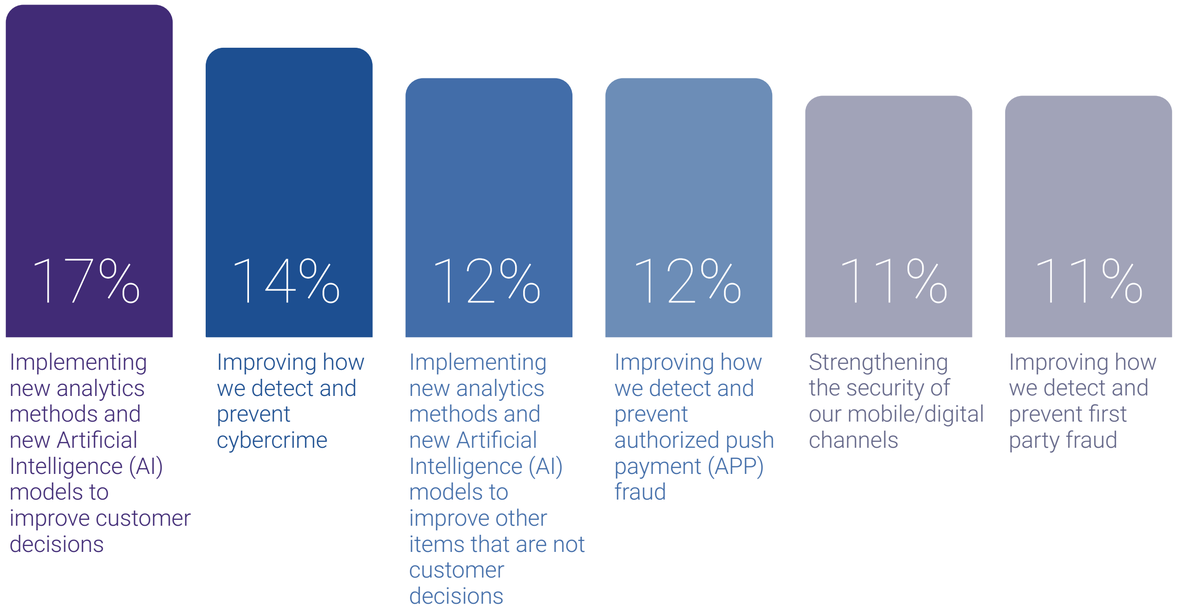
[11] https://www.ey.com/en_us/insights/ai/productivity-potential-gen-ai

Moreover, detecting and preventing Gen AI fraud and deep fakes is tied with detecting and preventing cybercrime as the greatest areas impacting the health of businesses – both reported by 17% of businesses. And businesses know this stress isn't going away anytime soon. Looking to the next 2-3 years, AI fraud is expected to be the second greatest challenge for businesses (70%). And despite high concern, confidence in being able to address generative AI fraud is low, as the second lowest confidence, coming in at 11th on the list of 12 at 77%.

It's clear businesses are concerned, even stressed by the idea of GenAI fraud, however, they don't seem to be prioritizing funding resources to identify or prevent it. When asked about initiatives they were actively pursuing in 2024, preventing and detecting GenAI fraud and deepfakes came in 9th on the list.

Furthermore, when asked about the most important potential investment areas for 2024, detecting and preventing GenAI fraud and deepfakes didn't make the top 5, it didn't even make the top 10! Preventing GenAI fraud came in 12th on the list of most important investment areas, at 8%, behind detecting and preventing identity theft, first-party, synthetic identity fraud, and other legacy fraud types, in addition to initiatives directed more at customer experience.

**Table 10:** Most important investment areas for 2024

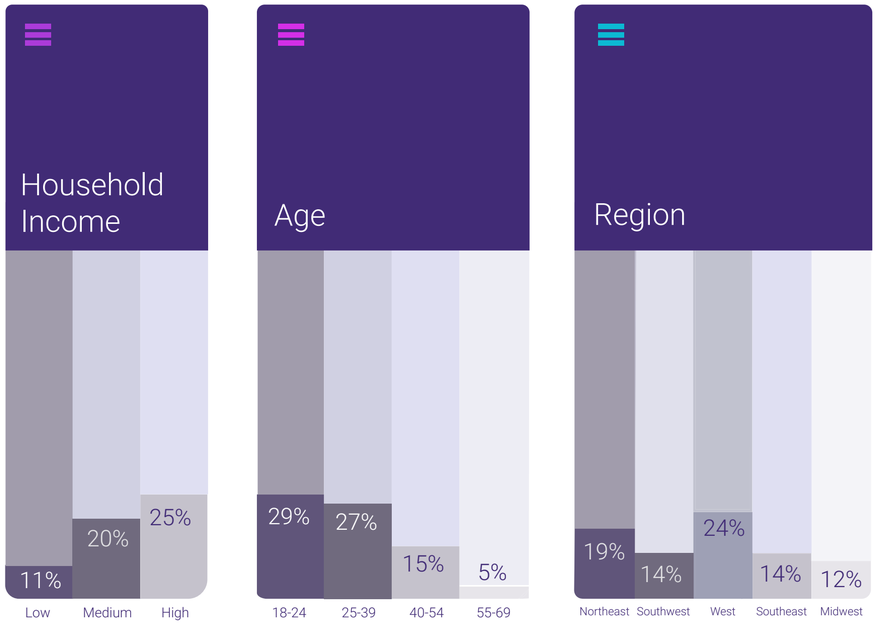



## Putting your money where your stress is

It's safe to say, GenAI is not only changing the way we work, but also the way we live, learn, and play. Consumers are not only taking notice of GenAI but dare we say it, they're excited.[12] They're observing the benefit GenAI is having in the workplace, but reactions are mixed when it comes to using it in everyday life, with concerns around ethics and the potential future effects of its use.

Consumers in our survey seem a bit slow to adopt GenAI, with 17% reporting using AI-driven chatbots like ChatGPT. While still low, there are some notable spikes in comparative usage across age, income level and region: 25-39 year olds (27%), high-income users (25%), and consumers in the West (24%).

**Table 11:** AI-Driven Chatbot Usage by age, income level and region




# Excitement about GenAI does not equal adoption with consumers

In looking at more recent adoption, only 10% of new account openings in the last six months were related to GenAI chat programs like ChatGPT. AI-driven chatbot accounts are most likely to have been opened by 16% of 25-39-year-olds, while least likely by 3% of 55-69-year-olds.

Still, while adoption is still relatively low, recent studies show consumers in the U.S. tend to be ahead of other countries. A recent report from Forester[13] attributes this to regulatory constraints and general consumer attitudes toward the technology in other countries, and that much of the training data for large language models (LLMs) is in English. The report goes on to say that consumer reservations still exist namely around the accuracy of results and the ways companies are using the data that consumers submit to GenAI systems.

Interestingly, only 12% of consumers in this year's survey thought that programs like ChatGPT should protect them while they're online. This could be due to current adoption levels, but might also be attributed to a lack of awareness around the usage implications.

[12] https://www.bcg.com/press/24april2024-consumers-genai-in-the-workplace-and-daily-life

[13] https://www.forrester.com/report/the-state-of-consumer-usage-of-generative-ai-2024/RES180689

# _EXPERIAN PERSPECTIVE

Whether the adoption curve is steep or flat, businesses and consumers alike will continue to deepen their knowledge and use of the technology. And by design, the technology will return better, more accurate outputs over time. One thing is for certain, GenAI is no longer a trend but is here to stay.

Fraudsters have also seen the benefit in leveraging GenAI to conduct fraud on more widespread levels. Just as it does with businesses and consumers, the technology allows fraudsters to quickly create images, text, and video to create fake bank statements, IDs, duplicate company websites, and even deepfakes of company executives with their voice and likeness. Perhaps the most infamous yet occurred in early 2024 where scammers used GenAI to create digitally recreated versions of a Hong Kong company's CFO and other executives to transfer $25 million to fraudsters posing as the executives.[14]

It's clear GenAI can and already is supercharging criminals efforts to defraud businesses and consumers alike. Look no further than FraudGPT, the dark web counterpart of ChatGPT, purpose-built to enable fraud through GenAI. New capabilities like behavioral analytics will be integral to staying ahead of GenAI driven fraud. This technology relies on tracking behavior or how a person inputs data, i.e. clicking a box, editing a particular field, hovers over before clicking, etc., and other digital interactions. It can detect and predict if an individual's intent is malicious. Behavioral analytics isn't collected or tied to a single identity, which makes it challenging for GenAI to learn from, or impersonate or replicate behavioral data.

Meanwhile tried and true methods of fraud will still proliferate and GenAI will only make them easier to execute. Perhaps now more than ever, it's imperative that companies utilize a holistic approach to fraud that can prevent and detect and mitigate fraud attempts. Orchestration will be imperative in this new frontier of identity and fraud, so look for partners that bring together the most robust data and leading-edge partners in the areas of identity verification, fraud risk and authentication, to apply the right tool at the right time to prevent infiltration and exposure.

Businesses will also need to work with fraud prevention partners who are continuously innovating in the data, tools, and technology they use to confirm identities, identify threats and bad actors, and prevent fraud.

While GenAI has seemingly unlocked a vast amount of fraud vulnerabilities, it can also be a tool for good in the fight against fraud. It can create efficiency and effectiveness in fraud monitoring by analyzing large amounts of transactional data to detect any unusual patterns and identify possible fraud. In addition to identifying fraud more quickly, it can also help in reporting that fraud or suspicious activity more promptly as well.

It can also help drive innovation. "At Experian, we champion the responsible use of generative AI to accelerate new product and service innovations, drive operational productivity, increase financial inclusion, and foster a flexible, adaptive approach to using the technology," said Kathleen Peters.

Companies interested in leveraging GenAI should start with forming a risk committee or having your risk committee take GenAI under consideration. This group will help define your organization's risk tolerance for GenAI usage and also ensure safe, responsible and ethical use of the tool. Next, look for opportunities to implement GenAI into your systems, typically those that could benefit from improved automation and increased productivity. And finally, ensure you are educate your employees and stakeholders on what your doing and your progress, all the while keeping your risk committee engaged.

[14] https://www.cnbc.com/2024/02/14/gen-ai-financial-scams-are-getting-very-good-at-duping-work-email.html

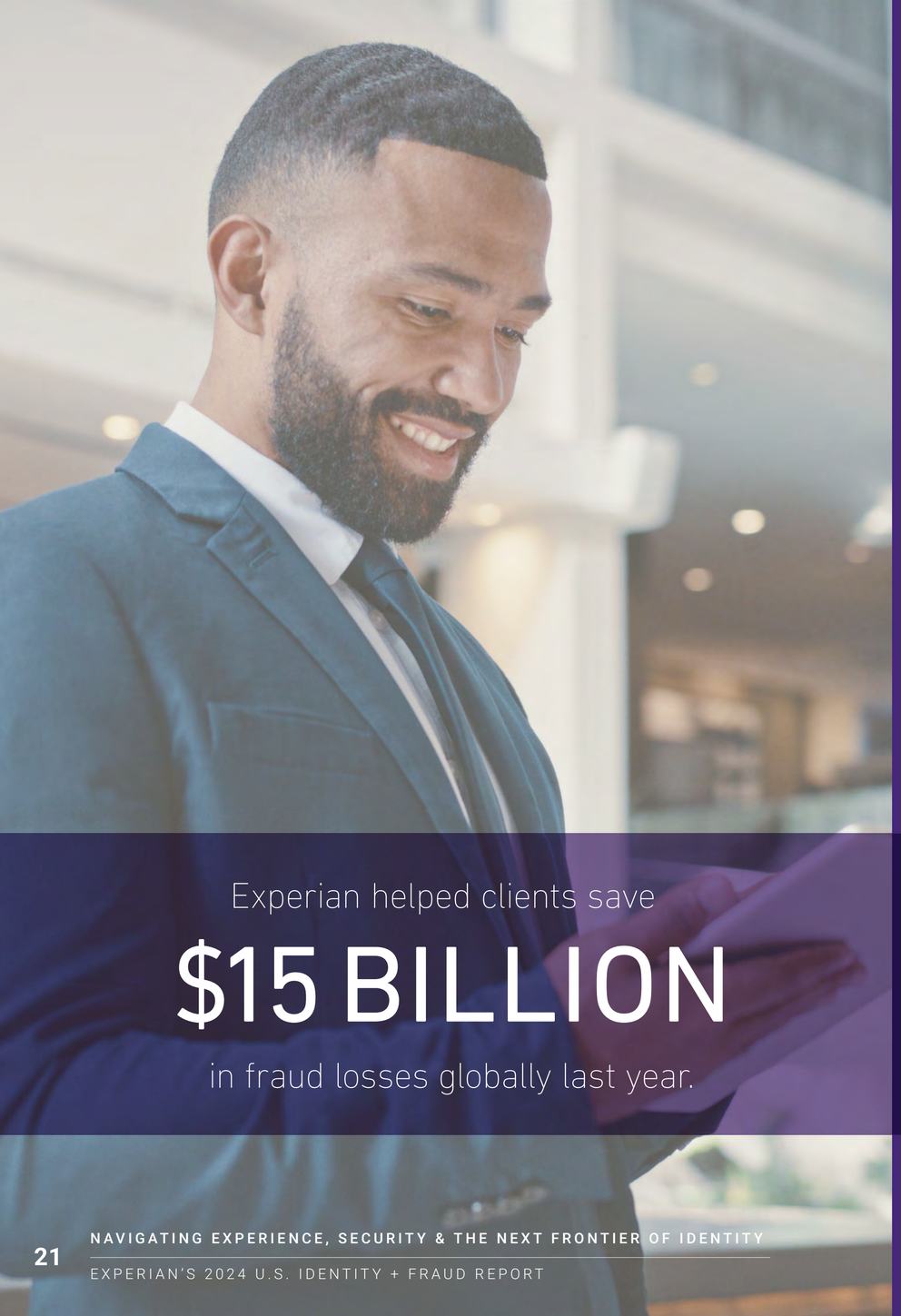
# Your partner in bringing together data, identity and next generation fraud prevention tools

We continue to observe higher incidences of account takeover, identity theft, APP fraud, and fraudulent new account openings, and businesses are significantly increasing their fraud prevention investments in response. At the same time, almost all businesses seem to be more focused on growing their portfolios, with their online identity strategies focused on security customer experience, the ability to digitally recognize their customers, and analytics related to customer decisioning. With the stress of cybercrime as a top concern, businesses seem aware of the growing threat of GenAI fraud, but stopping it is lower on their priority list at this time.

With consumer trust waning, businesses will need to continue to focus on strategies that build trust. In particular, greater investments are needed in the security technologies that allow all customers to be repeatedly identified and authenticated quickly, accurately and conveniently, all of the time. Moreover, businesses should communicate with consumers about the ways they're keeping them safe.

Additionally, organizations will need to continue to expand their investments in ML-driven solutions that can detect and prevent new fraud threats in real-time. Moreover, advanced technologies like behavioral analytics will be foundational not only in confirming customers with good intentions but also in stopping Gen-AI-powered fraud attacks.

Preventing fraud and providing a delightful customer experience aren't binary and shouldn't be opposing aims. But that's often how they're viewed in the marketplace. Companies shouldn't have to choose between protecting their systems and their customers and bringing good consumers into their business. And with Experian, you don't have to. We are committed to providing our clients with the world-class data, analytics and technologies designed to prevent fraud while providing the best customer experience. We are continually innovating and investing in solutions that amplify our fraud risk suite so companies can focus on growth. It's how we helped our clients across the globe save $15 billion in fraud losses last year.



Experian helped clients save

**$15 BILLION**

in fraud losses globally last year.

# HOW EXPERIAN CAN HELP

Fighting fraud while providing a frictionless, delightful customer experience requires a modern, intelligent and holistic approach. Businesses are facing mounting challenges – from first-party fraud and credit washing to synthetic identity and the growing impacts of generative AI-powered fraud. From increases in direct deposit account and check fraud, as well as advanced technologies like deepfakes and AI-generated phishing emails, consumers are increasingly at risk from sophisticated fraud schemes. It's now more important than ever that businesses apply a multilayered approach that can prevent fraud, confirm identity, and provide a positive customer experience.

Experian's suite of fraud and identity solutions was designed to do just that, purpose-built by a team of experts with decades of fraud prevention experience.

Our award-winning solutions go beyond traditional orchestration with true integration to increase operational efficiencies while solving your business problems related to fraud risk, identity verification, authentication and any other part of the customer lifecycle. These industry-leading tools leverage deep domain expertise and advanced analytical capabilities to interpret data to find bad actors while preserving the customer experience for good customers. Moreover, we are not only focused on solving the market problems of today, we are also continuously innovating and investing in advanced technologies and new data sets to future-proof your fraud strategy. Experian uses adaptive, advanced fraud management and identity verification strategies that can help you stay ahead of increasingly sophisticated fraud tactics.

RETURN TO CONTENTS

Experian is the world's leading global information services company. 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 prevented $15B in fraud losses globally. And we would love to help you.

Click here to learn more.

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