IDENTITY, EXPERIENCE AND THE EVOLVING FRAUD LANDSCAPE

Experian's 2023 U.S. Identity + Fraud Report

CONTENTS

RETURN TO CONTENTS

INTRODUCTION

After a resilient showing in 2022, the U.S. economy seemed to enter 2023 facing some headwinds. The first part of the year brought increased geopolitical turmoil, volatility in the banking system, rising interest rates, and higher prices creating an unpredictable and challenging atmosphere that's likely to impact business investment and consumer spending in subsequent quarters. 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 emerge 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?

Experian's 2023 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.

ABOUT THE RESEARCH

The 2023 Experian Identity and Fraud Report marks the eighth year of the study. The report is based on two major surveys conducted in the U.S. in March of 2023. 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 North America** 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 bank, fintech, consumer technology and electronics, payment system provider, and many other companies from a range of verticals.

RETURN TO
CONTENTS

Market conditions keep security and fraud at top of mind for consumers and businesses

MARKET CONTEXT

Fraudsters are opportunistic criminals and 2022 and the first few months of this year brought opportunities like never before. This volatility perpetuated an unpredictable atmosphere for both businesses and consumers alike.

Meanwhile, the rapid growth of technology adoption continues to drive increased digital transactions, and criminals have found new ways to exploit vulnerabilities, while also returning to tried and true tactics. The impact has been harrowing for consumers, who reported losing a total of $8.8 billion last year, according to the Federal Trade Commission.[1] This was an increase of more than 30 percent over the previous year, and doesn't take into account losses that went undetected or unreported. These all add to the more than $43 billion in total losses due to identity theft and fraud in the U.S. in 2022.[2]

But consumers weren't alone in feeling the effects of fraud. According to a recent PwC survey, over half of companies with global annual revenues over $10 billion experienced fraud during the past 24 months and nearly 1 and 5 reported that their most disruptive incident had a financial impact of more than $50 million.[3]

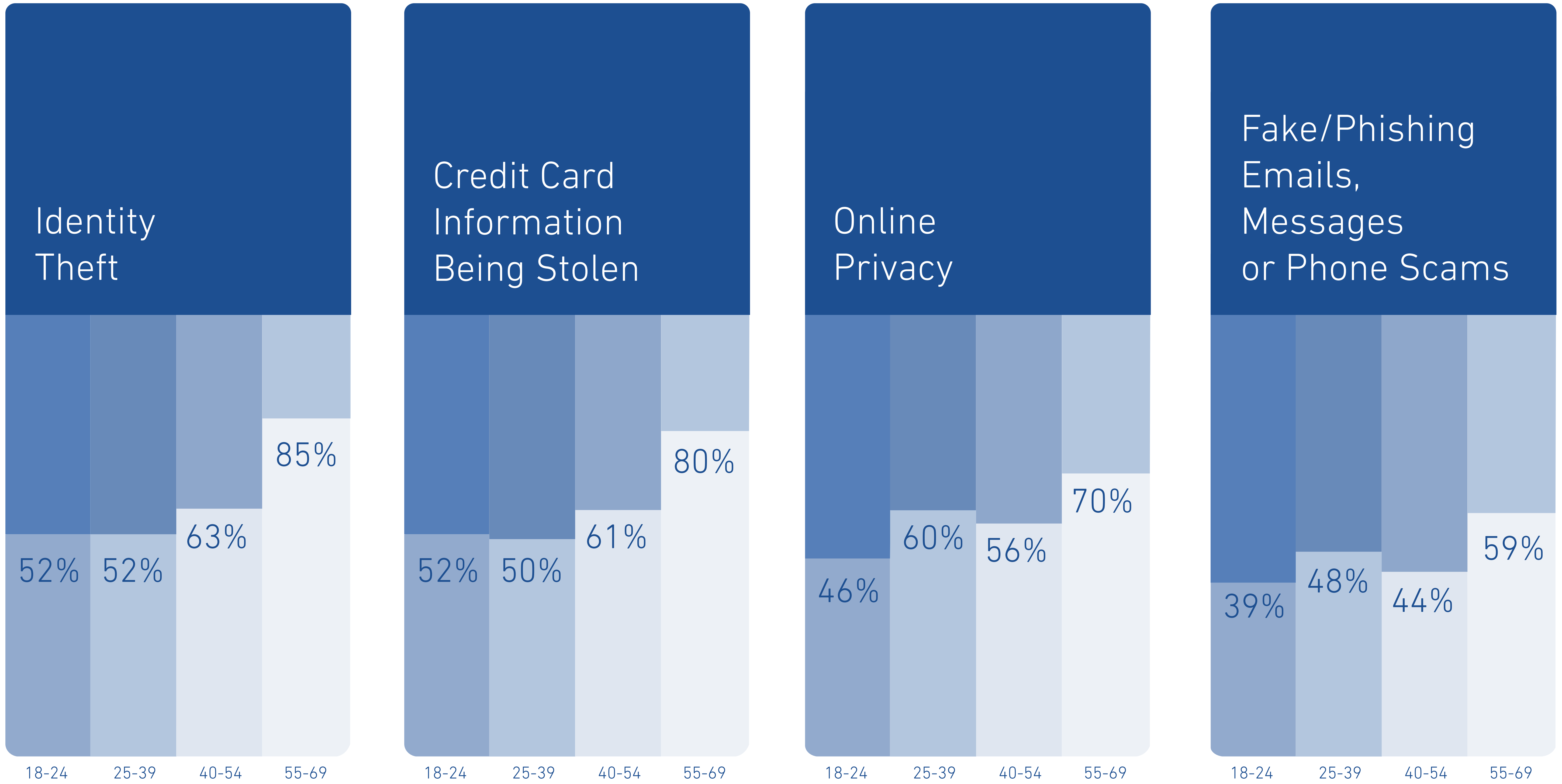
[1] https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022
[2] https://javelinstrategy.com/press-release/identity-fraud-losses-totaled-43-billion-2022-affecting-40-million-us-adults
[3] https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

RETURN TO CONTENTS

CONSUMER SNAPSHOT

Considering the widespread implications of fraud, it's no surprise that this year's research shows that over 52% of consumers feel like they're more of a target for online fraud than they were a year ago. As such, online security continues to be a very real concern for most consumers. Nearly two-thirds (64%) of consumers say that they're very or somewhat concerned with online security, with nearly one-third (32%) saying that they're very concerned.

Table 01: Consumer concerns by fraud type and age category



The research also reveals the primary fraud types are of the highest concern in the older age categories, most notably, 85% of 55-69 year olds are concerned by Identity Theft.

Nearly two-thirds

64%

of consumers say they're **very or somewhat concerned with online security**

Furthermore, consumers listed identity theft (64%), stolen credit card information (61%) and online privacy (60%) as top concerns when they're conducting activity online.

However, fake and phishing emails, false information, crypto scams and romance scams — which all potentially fall under the category of Authorized Push Payments (APP) fraud — are all strongly represented as pressing consumer concerns.

Notably, consumers aged 55–69 tend to be significantly more concerned with fraud.

RETURN TO CONTENTS

BUSINESS SNAPSHOT

Fraud is certainly on the radar for most businesses with nearly 50% saying they discuss it often and 31% saying it's always discussed. Moreover, 75% of businesses surveyed reported being confident in their ability to protect against all types of fraud. Interestingly though, less than half (45%) reported that they fully understand the impact that fraud is having on their business.

Still, survey results show that resources are actively being allocated in 2023 to try to minimize the impacts of fraud. Just over 50% of businesses overall report a high level of concern about fraud risk, with leading areas of concern including transaction fraud, cybercrime and identity theft.

Table 02: Fraud concern by sector

RETAIL BANKING	52%
FINTECH	58%
DIGITAL-ONLY RETAILER	36%
CLICK + MORTAR RETAILER	47%
CONSUMER TECHNOLOGY + ELECTRONICS	56%
TELECOM PROVIDER	40%

The concern is warranted with the greatest proportion of businesses, nearly 70%, reporting that fraud losses have increased in recent years. Almost 60% of digital-only retailers (58%) say they've experienced "somewhat more" losses.

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

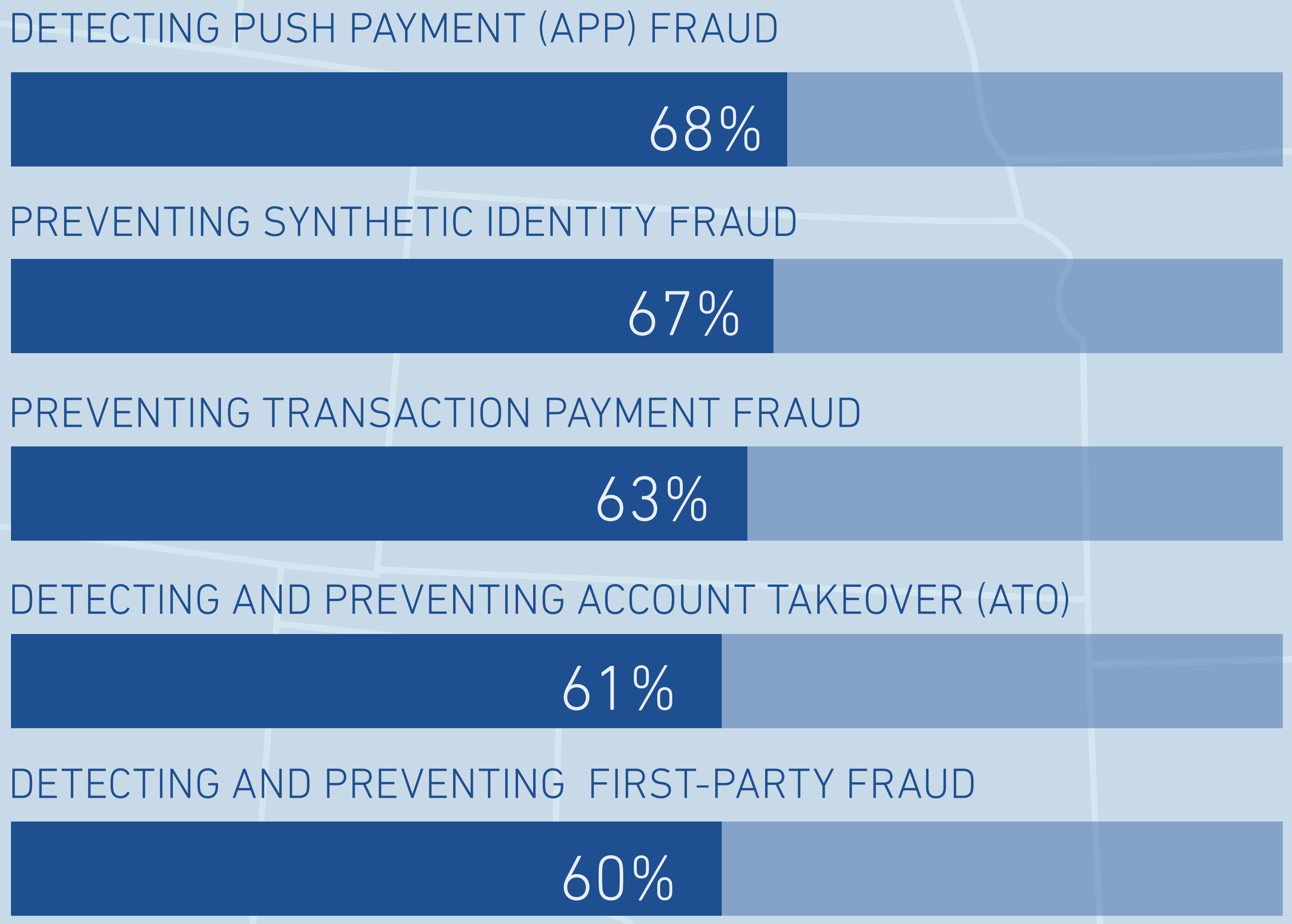
AUTHORIZED PUSH OR WIRE TRANSFER PAYMENT (APP) FRAUD	41%
TRANSACTIONAL PAYMENT FRAUD	38%
ACCOUNT TAKEOVER (ATO)	33%
FIRST PARTY FRAUD	33%
IDENTITY THEFT	33%
SYNTHETIC IDENTITY FRAUD	33%

RETURN TO CONTENTS

For 2023, APP continues to be the leading fraud event experienced by 40% of businesses, followed closely by transactional payment fraud at 34%. APP fraud involves a fraudster deceiving a consumer, persuading them to willingly deposit funds into the fraudster's account, or to the account of one or more complicit third parties (money mules). APP often includes social engineering of the victim using fake investment schemes, impersonation scams, purchase scams or other such schemes.

As such, businesses report they're prioritizing investments in the areas of APP detection; first-party fraud prevention, which increased in priority from last year's report; and synthetic identify fraud.

Table 04: Top fraud prevention priorities for U.S. businesses



EXPERIAN PERSPECTIVE

Businesses and consumers continue to be aligned when it comes to their concerns about fraud risk. For businesses, however, growing APP fraud risks, along with persistent synthetic identity and first-party fraud risks, require companies to use a layered approach that leverages multiple types of recognition and security.

RETURN TO CONTENTS

Consumer expectations for security and experience continue upward path

RETURN TO CONTENTS

MARKET CONTEXT

As business concerns around fraud rise, so does investment. Most businesses report they plan to increase their fraud management budgets by at least 8% to as much as 19%. However, despite increasing their budgets for fraud prevention, businesses' current security measures don't seem to be in line with consumers' evolving expectations.

Case in point: 85% of consumers report physical biometrics as the most trusted and secure authentication method they have recently encountered, but the measure is only currently used by 33% of businesses to detect and protect against fraud.

More evidence of this disconnect is the fact that passwords, security questions, account usernames and contact information round out the list of the top five methods currently encountered by consumers during account opening processes. However, only one of these methods (security questions), features in the list of consumers' most-trusted solutions.

When it comes to security and experience, the gap between consumer expectation and business execution may seem narrower this year.

While more than half (52%) of U.S. businesses are planning to ramp up investments in security measures that require customers to have a device in hand, they also seem to be hearing consumers, with 32% saying they'll also be investing in physical biometrics solutions to detect and protect against fraud.

Table 05: Top 5 measures currently used by businesses for detecting + protecting against fraud

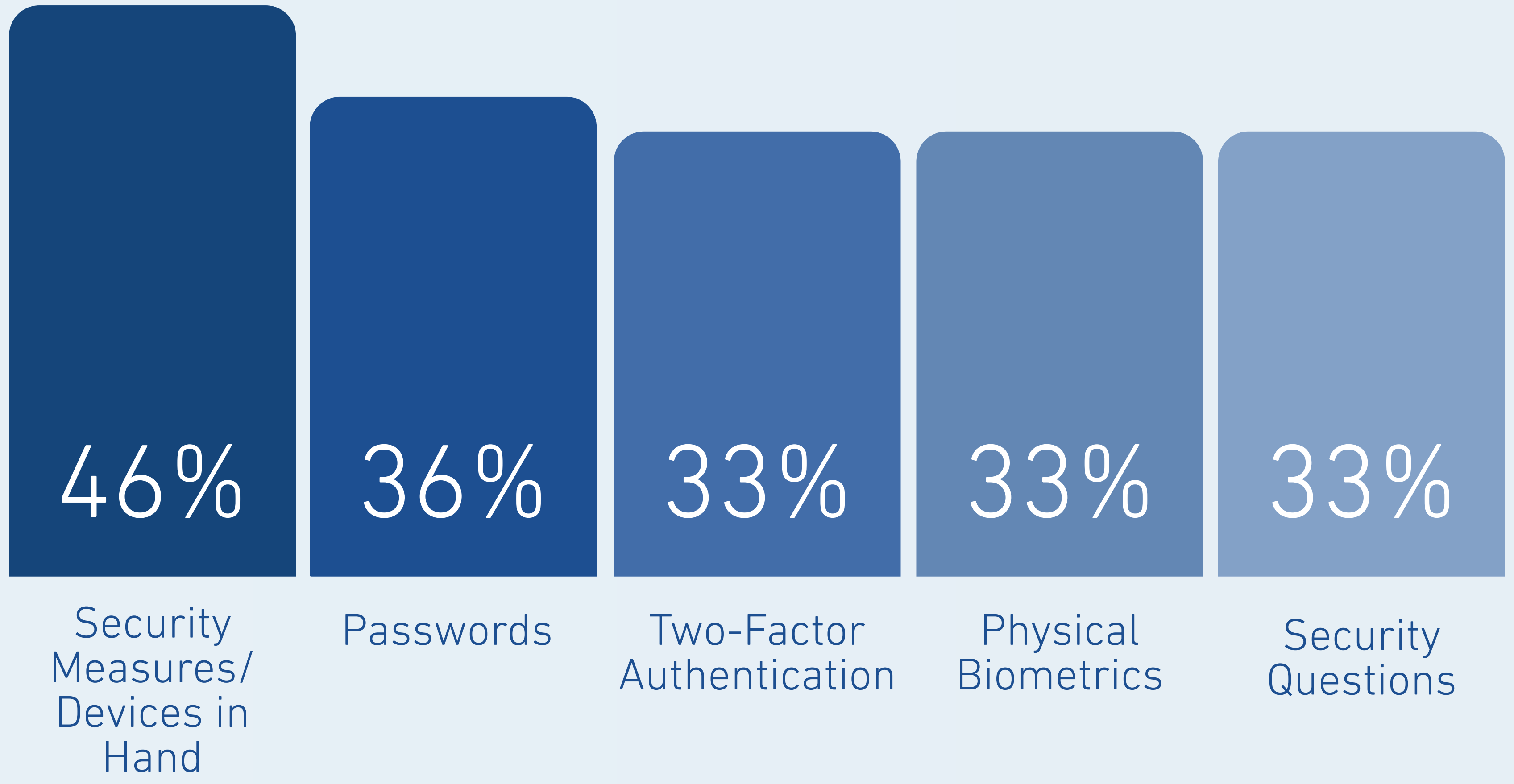


Table 06: Top 5 measures that make consumers feel most secure

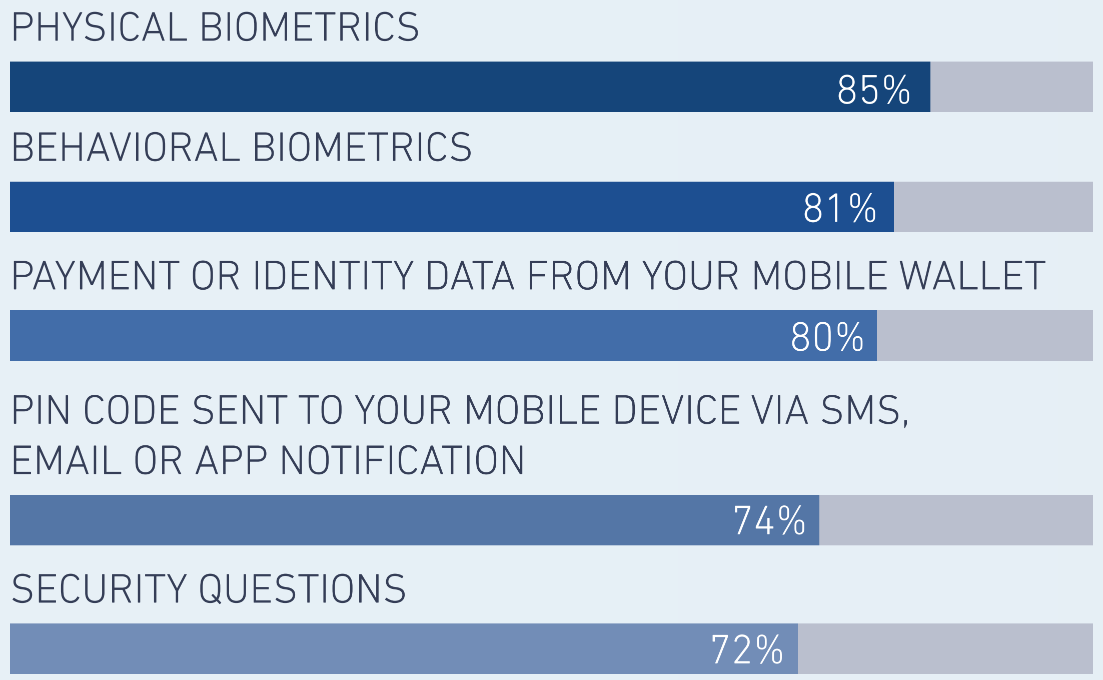
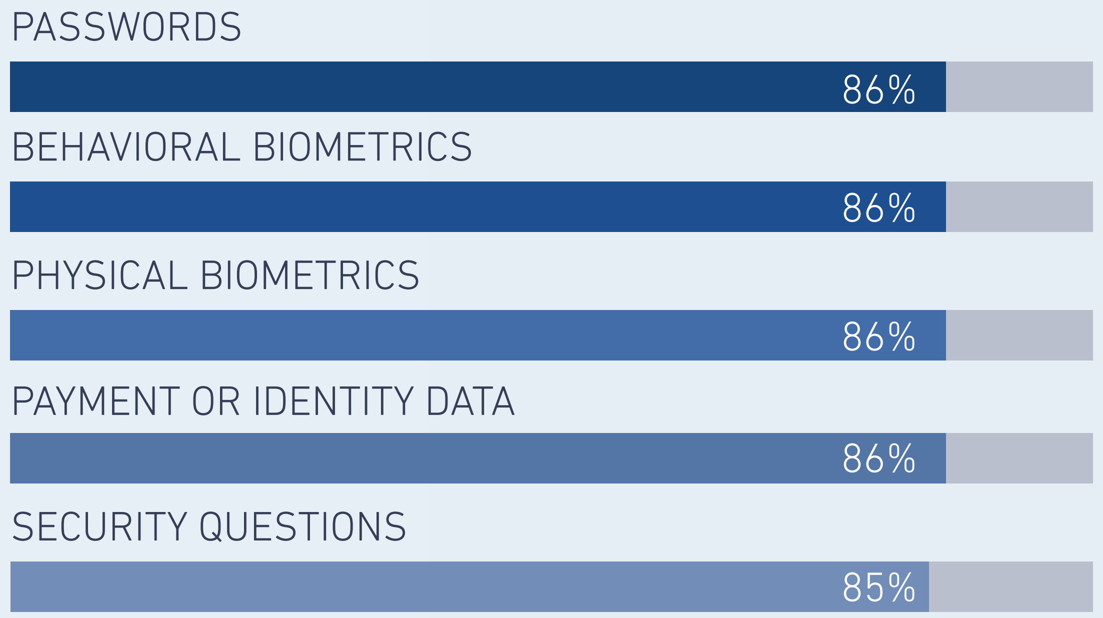
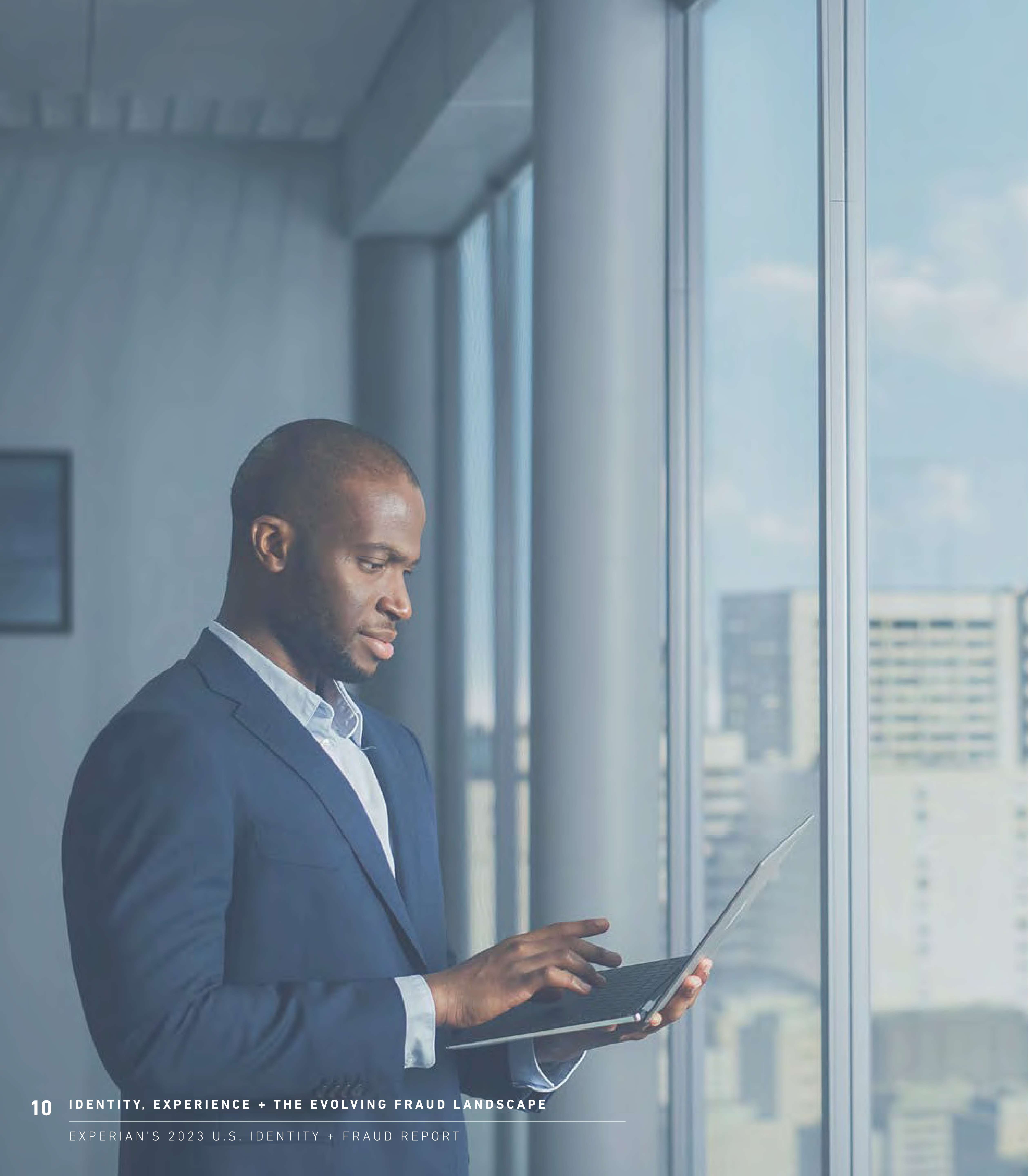


Table 07: Top 5 measures consumers say are important to a better online experience



For the most part, consumers seem to agree that the security measures that make them feel most secure can also create a better online experience.

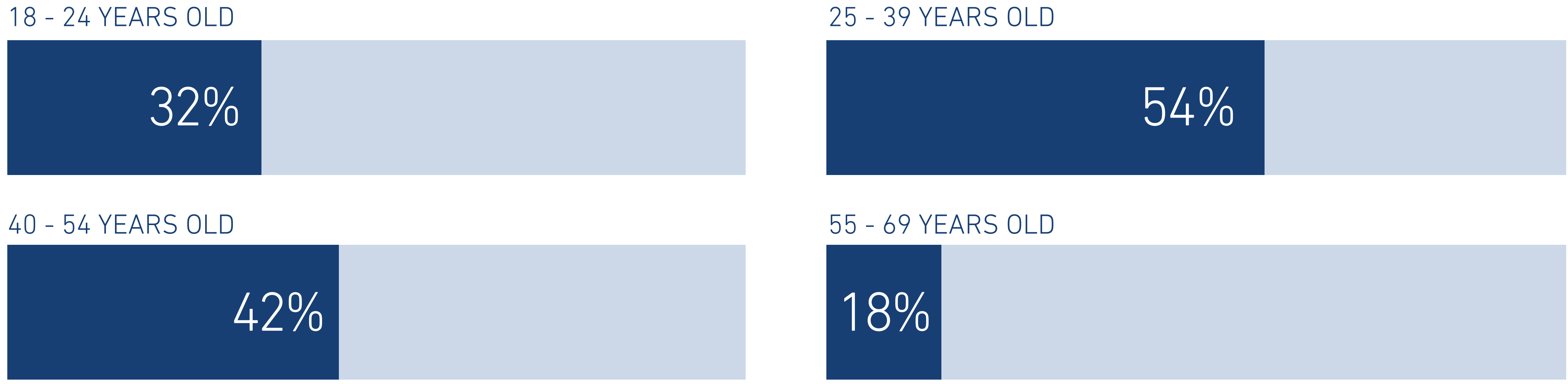


UNHAPPY CONSUMERS VOTE WITH THEIR MOUSE AND THEIR FEET

Despite concerns around fraud and online security, 55% of U.S. consumers reported setting up a new account in the last six months, with consumers in high-income households (80%) and 25–39 year olds (73%) reporting the newest account openings. The highest account openings were reported for streaming services (43%), social media sites/apps (40%) and payment system providers (39%).

However, the new account opening experience wasn't as rosy for everyone. Significantly, 51% of U.S. consumers considered ceasing account opening during the process due to friction and a less-than-positive experience. This was highest among high-income households (69%) and those aged 25–39 39 years-old (60%).

Table 08: Breakdown of consumers, by age, who have moved their businesses elsewhere due to a negative account opening experience



However, the disconnect between consumer expectations and current identification and authentication methods is having a significant and measurable impact on abandonment rates in new account opening processes, with 37% of consumers moving beyond consideration to action and taking their business elsewhere due to a negative experience. Again, this was highest among high-income households (62%) and those aged 25–39 years old (54%).

RETURN TO CONTENTS

CONSUMER SNAPSHOT

It's clear that consumers have high expectations for security and a positive experience with the businesses they deal with.

More than 85% of consumers expect businesses to respond to their identity and fraud concerns, and these expectations have risen over the past several years. Consumers are also clear on the kinds of technologies and experiences they trust and consider optimal.

However, the seeming mismatch between consumers' wish lists for online identification and security — and the experiences they encounter in the real world — is leading to reduced satisfaction and increased abandonment during new account opening processes.

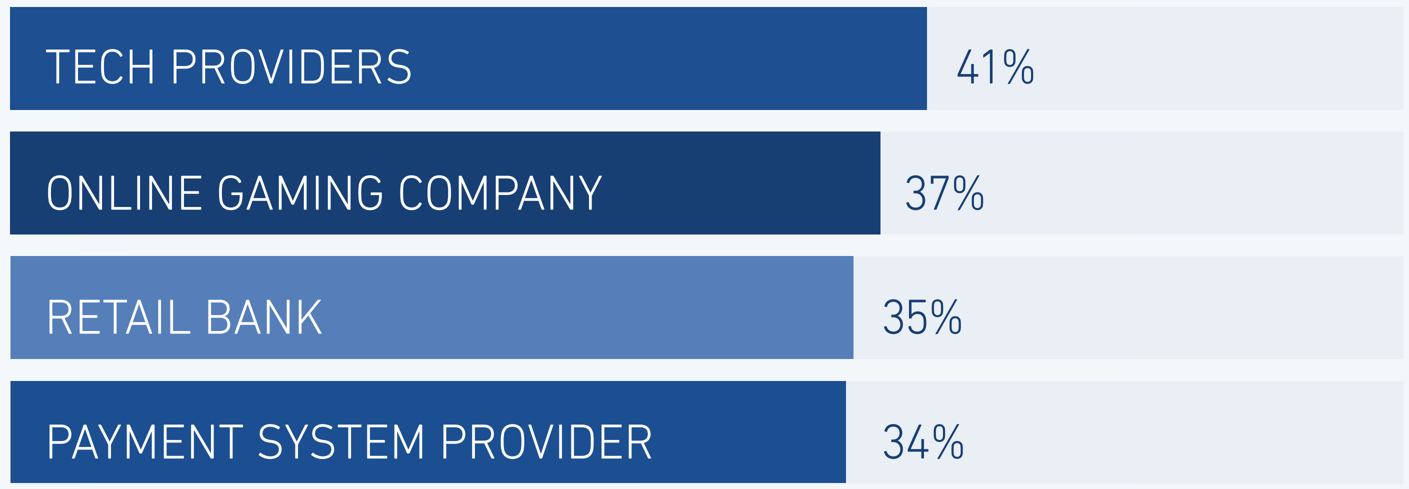
However, there's good news: consumers (67%) were surprisingly open to sharing their personal data. The data suggests that they see value in sharing their personal data, in that it improves their online experience, making it easier and more convenient to do business online, and helps to provide a more personalized experience.

The willingness to share data with businesses that are trusted and where they have a relationship has been trending upwards from previous years. Unsurprisingly, U.S. consumers very much like the idea of control as it relates to their personal data and how it's used by businesses, with 90% wanting more control (some/complete) and 61% wanting 'complete control' over their personal data and how it is being used.

BUSINESS SNAPSHOT

These findings, more than any other aspect in this report, demonstrate the scale of the challenges faced by businesses in terms of optimizing their identity and fraud-prevention strategies.

Table 09: Breakdown the most trusted businesses by segment



While some key investment priorities — such as physical biometrics — are totally in line with consumer preferences, each organization needs to carefully review its strategy to ensure that investments in new identity and fraud solutions can minimize abandonment rates and other measures of consumer dissatisfaction while simultaneously detecting and preventing fraud.

Our latest research shows when it comes to online activities and transactions, tech providers, online gaming companies and retail banks elicit the most trust from the highest percentage of consumers.

EXPERIAN PERSPECTIVE

Today's consumers aren't willing to compromise on digital customer experience and online security. We've found that customer expectations are evolving extremely quickly and that businesses who can keep up will be able to achieve new competitive advantage and deeper levels of market trust. However, achieving this will require a layered approach to fraud that identifies and treats the various fraud types appropriately, seamlessly letting good consumers through. This will necessitate targeted investments in Machine Learning (ML) driven technologies that can significantly improve online security and customer experiences as well as prioritization of the security technologies that consumers trust most — namely, physical and behavioral biometrics.

When it comes to online identification, 71% of consumers say it's very or extremely important for businesses to be able to accurately identify them online. Businesses are listening and seem to be well aligned. For example, 92% of businesses have a strategy in place for identifying consumers online, and 87% are confident in their ability to achieve it — up from an average of 84% last year. At the same time, however, many U.S. consumers (63%) are only either "somewhat confident" or "not very confident" in businesses' ability to accurately identify them online.

For those businesses who get it right and are able to consistently and accurately identify a customer online, the investment pays off, as there's a clear relationship between the ability of a business to successfully identify consumers online and consumer levels of trust in that business. This is very evident in the United States, where over 50% of consumers say that they trust (either very or extremely) an organization that can successfully identify them online.

Notably, high-income U.S. households (48%) indicate "extremely" trusting in this circumstance. Likewise, 25–54 year olds are also much more trusting of businesses that identify them online. Further, over 60% of consumers value and have confidence in businesses that have the ability to accurately identify them regularly and thoroughly online.

Machine Learning (ML) is now integral to fraud prevention

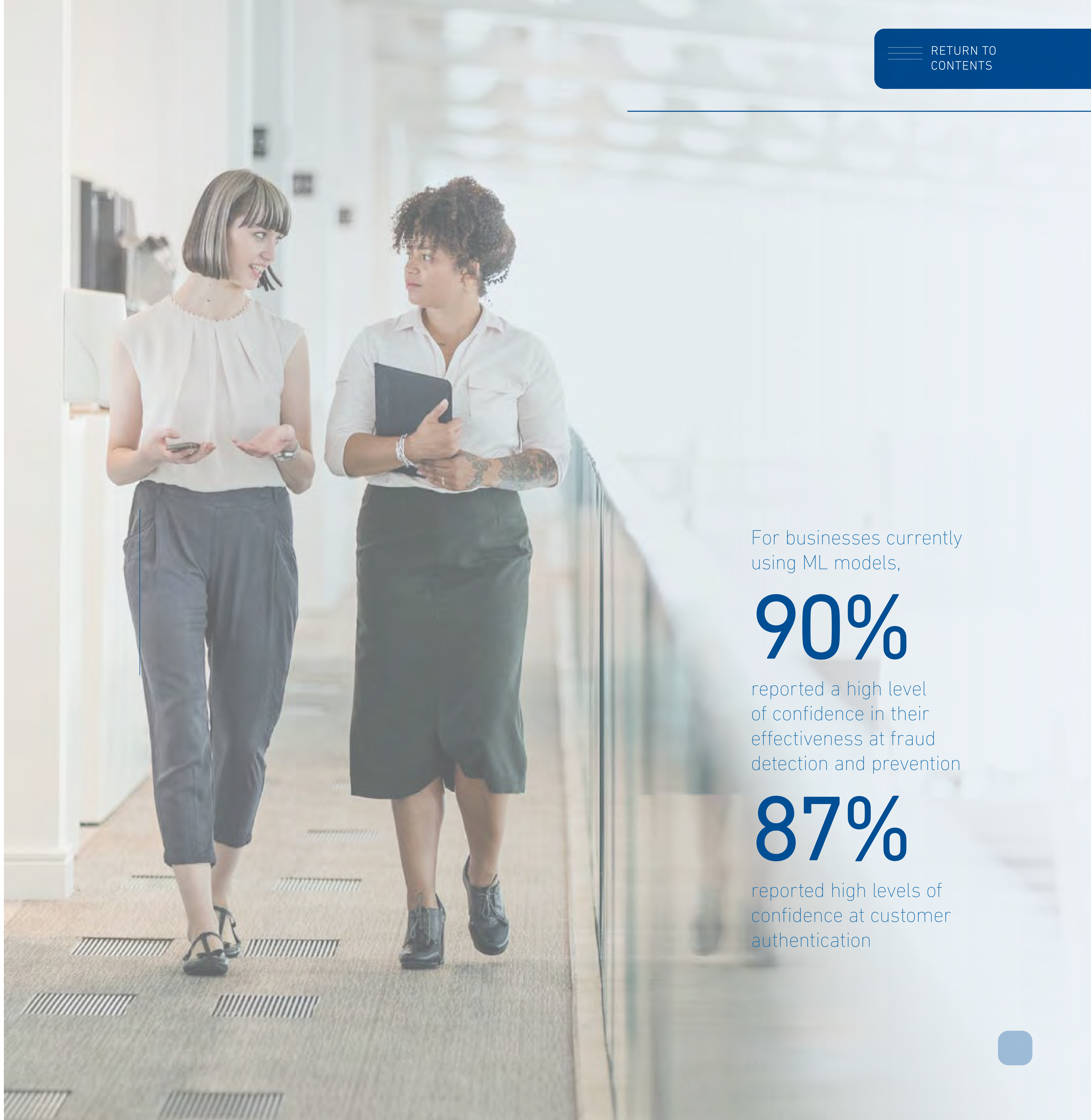
The evolving fraud and risk landscape requires that businesses use multiple types of recognition and fraud management solutions. However, a large majority of organizations still use rules-based analytics models to identify and flag incidences of suspected fraud. With fraudsters continually innovating and perpetrating new types of attacks, static models quickly become obsolete, increasing the risk of fraudulent transactions, data breaches and regulatory noncompliance — not to mention costs associated with these risks.

To address all these issues in 2023, nearly 60% of businesses are already emphasizing or are looking to build ML capabilities into their fraud identification and prevention strategies. ML is far superior to rules-based fraud models as the technology identifies both known and unknown trends in large data sets. When a new fraud trend or type emerges, the ML model is able to identify it and immediately flag it to the security team for further investigation.

The other benefit of ML is that large numbers of transactions or large data sets can be analyzed automatically, extending fraud prevention measures across the entire customer portfolio. This ensures that new and existing fraud risks can be identified quickly and at scale and that legitimate customers can continue transacting with their providers reliably, helping to enhance their online experiences.

For those businesses currently using ML models, 90% reported a high level of confidence in their effectiveness at fraud detection and prevention, and 87% reported high levels of confidence at customer authentication. ML models were one of the top solutions businesses said they're planning to add to their fraud prevention tool sets. While cost was listed as an obstacle for 25% of businesses to implementing ML models, a large percentage of businesses (35%) also cited "implementation complexity" and "unclear or conflicting internal decision processes" as the greatest difficulties associated with implementing ML models.

This suggests that many may still have their ML plans on hold as they wait for more easily integrated solutions and alignment on internal priorities. This delay is potentially worrying, particularly as traditional models are now incapable of keeping pace with evolving fraud threats. What's needed is a new generation of more efficient and scalable fraud solutions that have ML as a natively integrated component.



For businesses currently using ML models,

90%

reported a high level of confidence in their effectiveness at fraud detection and prevention

87%

reported high levels of confidence at customer authentication

RETURN TO CONTENTS

CONSUMER SNAPSHOT

As we've seen, security and privacy rank as consumers' top concerns in 2023. Not only that, more than 70% say it's extremely or very important for businesses to accurately identify them online. Based on its ability to automate and enhance both fraud detection and online customer identification, ML has now become an essential technology for businesses wishing to keep pace with consumers' growing security expectations.

BUSINESS SNAPSHOT

With nearly 60% of companies already prioritizing or planning to add ML-powered solutions to their identity and fraud portfolios, it's clear that the power of this technology to detect and prevent fraud is now well understood across all markets. However, implementation complexity is seen as a major barrier to those yet to adopt, suggesting a sizable segment of companies are still putting their ML plans on hold.

EXPERIAN VIEWPOINT

Experian® has long understood that ML will be a key technology for helping businesses to recognize and respond to both existing and new fraud threats. To make ML capabilities available to organizations in all verticals, we've built ML into several of our fraud prevention and data analytics solutions, dramatically reducing costs and ensuring that our customers can access fully trainable models that deliver accurate, timely fraud insights across their portfolios at scale.

"As fraudsters become more sophisticated and opportunistic, businesses need to proactively integrate the latest technology, data, and advanced analytics to mitigate the growing fraud risk," said Kathleen Peters, Chief Innovation Officer at Experian Decision Analytics in North America.

"Experian is making new investments and will continue to innovate and bring new solutions to market that help protect consumers and enable businesses to detect and prevent current and future fraud."

RETURN TO CONTENTS

Experian: Your partner in fighting fraud now and into the future

We continue to see higher incidences of synthetic identity, first-party and all types of APP fraud, and businesses are significantly increasing their fraud prevention investments in response. At the same time, almost all businesses are pursuing their online identity strategies focused on security and customer experience, to ensure that all customers can be identified and authenticated quickly, accurately and conveniently, all of the time. This year's report also highlights a gap between consumers' expectations for even more online protection and convenience, and business' ability to act and innovate quickly enough.

In particular, greater investments are needed in the security technologies consumers trust the most — including physical and behavioral biometrics. Additionally, organizations will need to continue to expand their investments in ML-driven solutions that can detect and prevent emerging, as well as new fraud threats in real time. Experian has helped businesses keep pace with the evolving fraud landscape and to deliver even more convenient, frictionless online experiences for consumers, helping clients save $11 billion in fraud losses globally last year.

Experian helped clients save

$11 BILLION

in fraud losses globally last year.

HOW EXPERIAN CAN HELP

APPLY A LAYERED APPROACH THAT IDENTIFIES + TREATS EACH TYPE OF FRAUD APPROPRIATELY

A one-size-fits-all solution doesn't exist. However, a layered approach allows businesses to modernize identity and keep pace with the ever-changing environment. Businesses need a framework that can reliably use different combinations of physical and digital identity data to determine that the person behind the identity is a known, verified and unique individual.

This is possible thanks to our end-to-end integration, orchestration and analytics capabilities, which provide real-time alerts for fraud risks, while ensuring that your legitimate customers can transact with you safely and reliably.

As well as reducing fraud risks, this can help you to provide a more streamlined, unified customer experience that minimizes abandonment during the onboarding process.

LEVERAGE INDUSTRY-LEADING DATA + ADVANCED ANALYTICS

Leveraging analytics wherever possible is crucial to streamlining decisions and choosing the right level of friction that's appropriate for the risk.

At Experian, we offer the rich data sources, advanced analytics capabilities, consultancy and services needed to rapidly adopt data analytics solutions that mitigate APP fraud risks.

Our solutions are used at some of the world's largest banks — to identify potentially fraudulent customers and transactions, and to ensure that action is taken in real time to prevent fraudulent payments being made.

RETURN TO CONTENTS

Experian works with the top financial institutions across the globe, helping them turn data into actionable insight. With a suite of fraud prevention and identity verification tools, we can help businesses detect and combat fraud, build trusted relationships with customers, assess risk, securely enter new markets, and address regulatory and compliance requirements.

We deliver an out-of-the-box, configurable environment for identity and fraud management that includes identity risk models, diverse authentication methodologies, verification checks, and layered orchestration and decisioning strategies.

Last year, Experian estimates that its fraud prevention solutions helped clients save $11 billion in fraud losses globally.

To discover more about our capabilities in this area, please visit our fraud management hub online. You can also contact us to discuss your specific security, fraud and identity requirements.

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