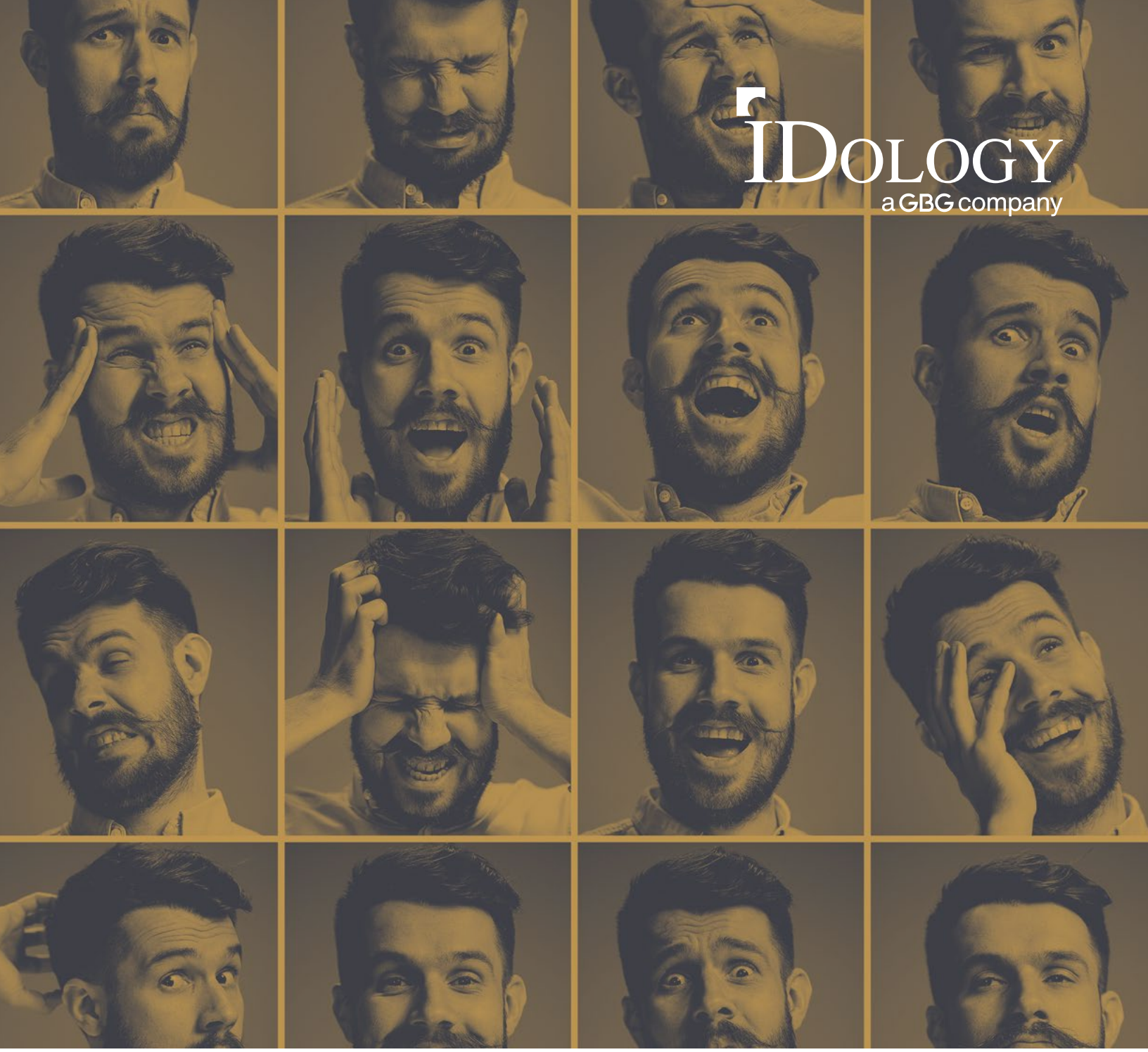


FIFTH ANNUAL CONSUMER DIGITAL IDENTITY STUDY

The Continuing Consumer Paradox: Delivering Security, Privacy & Convenience

TABLE OF CONTENTS

Methodology for our Fifth Annual Consumer Digital Identity Report:
Data for this report came from an online survey of 2,054 consumers collected in June 2022. Survey respondents are representative of the online U.S. population 18 and older, or around 253 million people.

INTRODUCTION

A Lack of Trust

Consumers have long embraced the convenience of engaging online, but the pandemic fast-tracked society's digital mandate. The demand for fast and convenient transactions has never been greater. Yet with more convenience comes more risk. The rapid increase in digital transactions has provided fraudsters with more opportunities.

Meanwhile, the consumer paradox continues. This year's findings show that consumers haven't fundamentally changed. Many things are still the same. Consumers still want convenient and frictionless transactions, including quick account openings and fast approvals. What has changed is a seismic shift in how consumers—and businesses—are responding to the environment around them, which is characterized by an abundance of competitive options, unprecedented fraud and an intolerance for anything less than a stellar customer experience.

Consumers increasingly want assurance that their transactions are secure and secured by the business they are interacting with. They are willing to bear some hurdles, but it must be just the right amount, and not too invasive. And while consumers expect personalized experiences, they are increasingly skeptical about the data they share and with whom. They are increasingly taking action to protect their data and safeguard their identities. And businesses are responding by delivering faster, easier and more secure digital experiences to protect against fraud, while safeguarding their most valuable asset—the customer relationship.

Consumers are also asked to provide personal information online so businesses can deliver on expectations for convenient and personalized customer experiences. But because they are increasingly skeptical about the data they share; they require reassurance that businesses are protecting them and their data. A lack of trust is understandable given the recent history of numerous high-profile consumer data breaches. Consumers are seeing more cyberattacks against the companies that hold their personal data, putting their own cybersecurity at risk.

With so much data in the hands of cybercriminals, fraud is an everyday occurrence for the American consumer—a reality of the post-pandemic economy where consumers shop and bank almost exclusively online. Data from the Federal Trade Commission shows that consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70% over the previous year. The most commonly reported category once again being imposter scams, followed by online shopping scams.[1]

Consumers hold a grim view of the future with **56%** expecting fraud attempts to increase (up from only 38% in 2021). In particular, 61% are concerned about the risk of malware on their smartphone. These concerns are not without good reason as an increasing number of individuals have fallen victim to fraud.

19% reported that they had a new account (such as a bank account, credit card or ecommerce account) opened in the last 12-18 months without their authorization. Furthermore, **17%** of those surveyed have personally been the victim of identity fraud during the same time period and faced the consequences of being exploited for financial crimes, including losing control of their bank account and the theft of a tax refund or health insurance information. Some even faced the issuance of an arrest warrant in their name, despite not being the perpetrator.

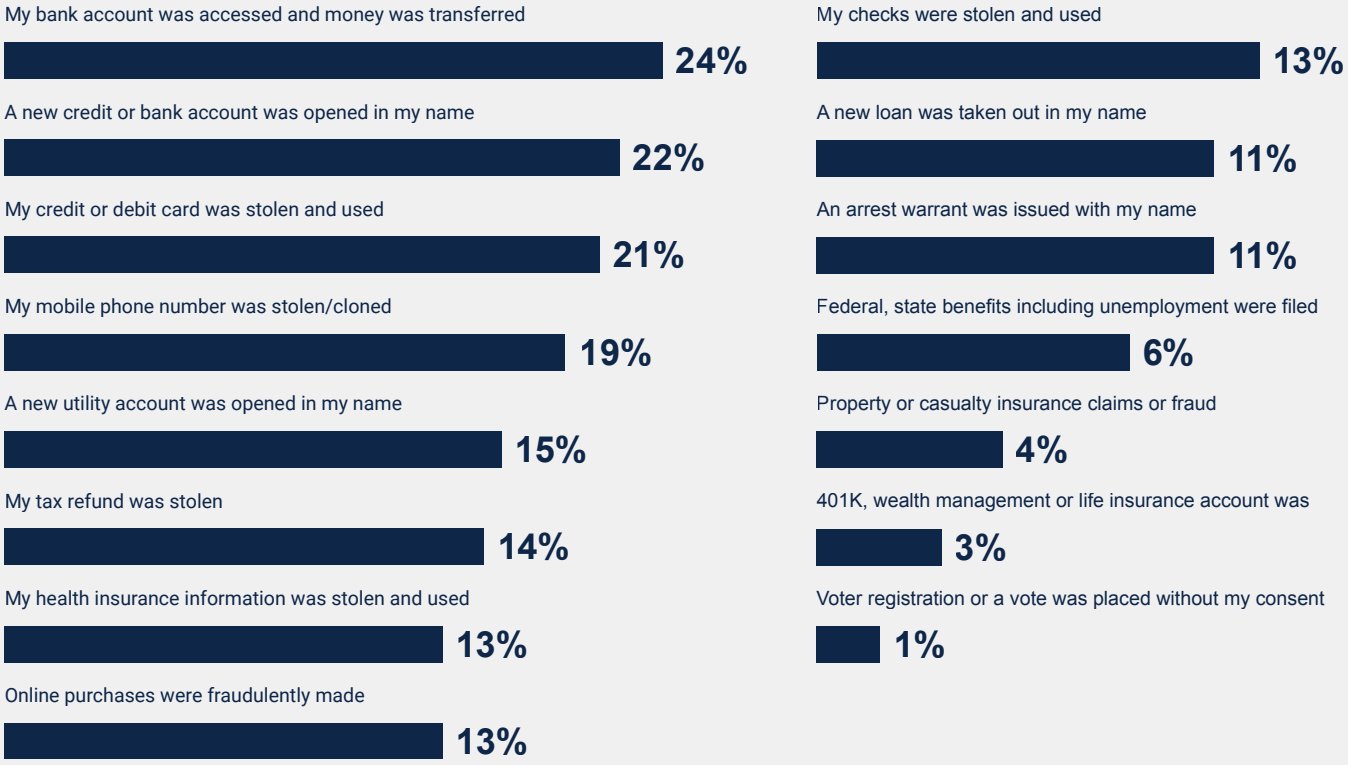
Do you expect fraud attempts to change over the next 12 months?

[1] https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

However, companies are investing in advanced identity verification to protect their business and consumers from the threat of fraud. In the last 12 months, **53%** of consumers report being required to provide further proof of their identity, such as submitting a photo of their ID via their mobile phone, when signing up for a new online account or using an existing online account.

This year's findings show that consumers want it all. In an environment where fraud attempts have surged to an all-time high, successful businesses must raise the bar on the digital experiences they deliver to consumers—providing easy access to the products and services they need, when and where they need them—while keeping security and trust in sharp focus. But as we will see, accomplishing this can be confusing to consumers.

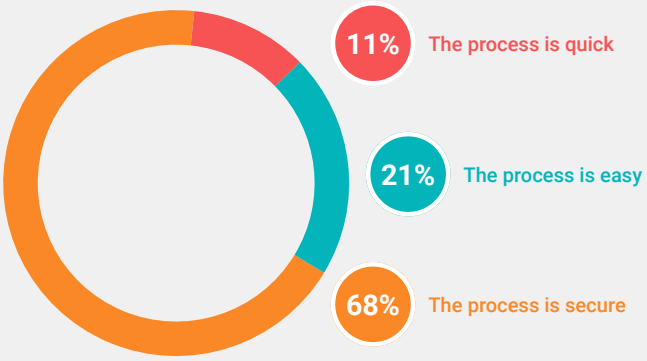
What happened when your identity was stolen?



Security vs. Convenience: There are No Compromises

Our survey found that **68%** of consumers rank a secure process as most important to them when opening a new account online, while in comparison, **32%** say that a quick and easy process is most important.

> When you open a new account online, which is most important to you?



This may seem straightforward, with security winning the day. But when it comes to consumer's actions, businesses cannot lose sight of how much consumers value ease and convenience. **45%** percent strongly dislike companies requiring additional security checks to determine if a high-risk transaction, such as a transfer or account change, is actually being made by them and not a criminal. And while elder age groups value secure processes, they are, ironically, more likely than younger age groups to strongly dislike additional security checks.

To further complicate things, **76%** report that if they knew an online company was using advanced identity verification, that knowledge would positively impact their decision or preference to use the company's services. And yet, **37%** percent have abandoned signing up for a new online account because the process was too difficult, too time-consuming or did not seem trustworthy.

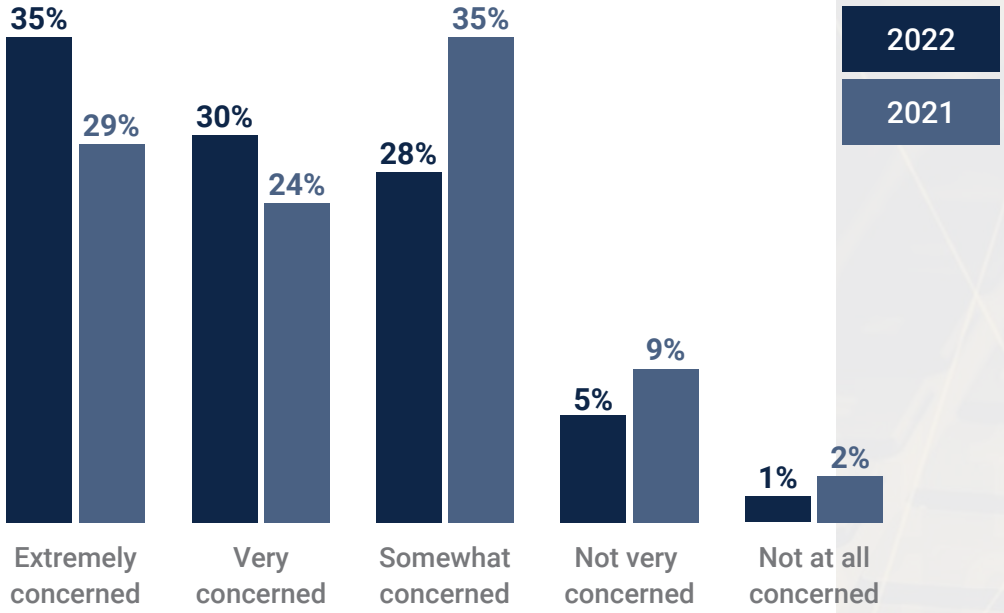
For all demographics, it's important to streamline the onboarding process—applying friction only when necessary. Consumers need to know that businesses are keeping them safe online, but not at the cost of convenience. Those organizations that get this balance right are better positioned to improve customer retention, increase loyalty and build stronger customer relationships for the long term.

Privacy & Data Protection: Consumers Hold Businesses Accountable

Due to the constant stream of data breaches, there's a heightened focus on the safety and security of personal data. In today's environment, whether a business focuses on privacy protection is a factor considered by consumers when asked to disclose personally identifiable information (PII). Furthermore, there has been a noticeable shift in consumer mentality when it comes to providing PII that doesn't seem relevant to the transaction—it feels intrusive.

When it comes to sharing personal information, **65%** are very or extremely concerned about companies collecting identity data online without their permission or knowledge.

How concerned are you about companies collecting your identity data without your permission or knowledge?

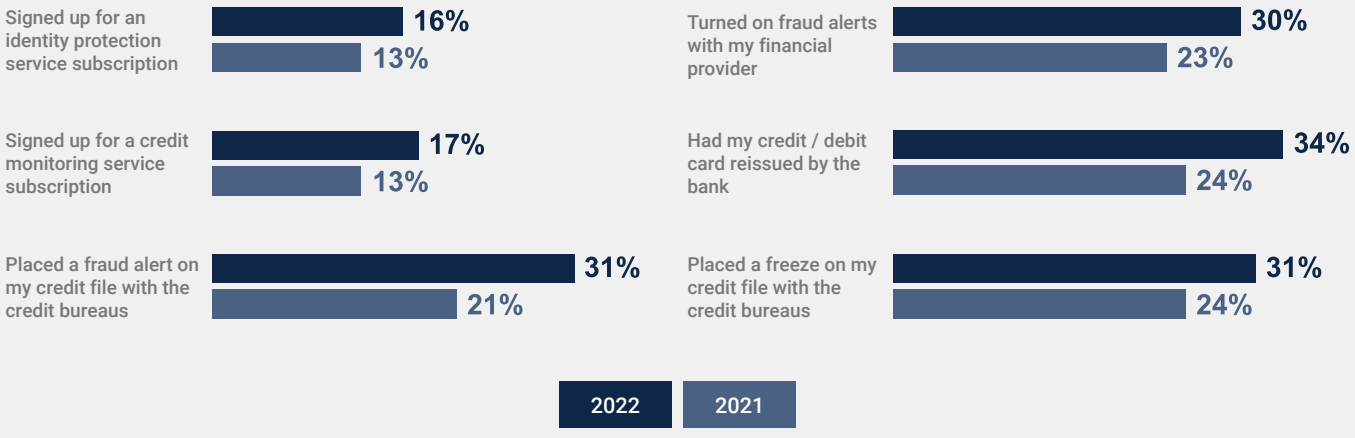


By only asking for information relevant to the task at hand, businesses are better able to build trusting relationships with consumers. Using this approach can signal to consumers that a company is taking a thoughtful approach to data management. Transparency is important, too. Some may feel it's okay for companies to collect data, so long as they are transparent about what they are doing with it.

Building on these findings, our survey also provides additional context to help businesses refine their approach to identity verification. We found that **67%** of respondents strongly agree it is the company's responsibility to protect their personal information. However, when asked if companies do enough to safeguard their personal identity information, **60%** said that they do not.

Consumers are increasingly aware of the importance of data privacy and are taking steps to protect their identity. **59%** percent of consumers report being more diligent in which accounts they open and the personal information they provide when opening accounts online. And when a breach happens involving their data, consumers are acting.

What steps have you taken to protect your identity since being notified that your personal information was breached?



While consumers are more engaged, further education is needed. **40%** are unsure if their personal information is currently available for sale to criminals on the internet. And **69%** of consumers do not know what synthetic identity fraud (SIF) is, one of the most insidious and the fastest growing type of fraud in the United States.

Synthetic Identity Theft Explained

Synthetic identity theft is a type of fraud in which a criminal combines real and fake information to create a new identity. The real information used in this fraud is usually stolen. This information is used to open fraudulent accounts and make fraudulent purchases.*

A synthetic identity is a combination of fabricated credentials where the implied identity is not associated with a real person. Fraudsters may create synthetic identities using potentially valid social security numbers (SSNs) with accompanying false personally identifiable information (PII).**

Data collected by IDology points to a recent surge in synthetic identity fraud. Unfortunately, those who often suffer the most from SIF are vulnerable populations, including minors, elderly, and deceased individuals. These demographics are vulnerable for different reasons, but they all have something in common. In addition to being vulnerable to SIF, our data shows that all three groups have seen a progressive increase in SIF rates.

Unfortunately, children are one of the biggest targets of SIF schemes. Research shows that more than 1 million children experience identity theft annually, and two-thirds know the perpetrators. Thankfully, **44%** of those surveyed report taking steps to monitor or safeguard their child's identity. Seniors, college students, spouses, significant others and online daters are also targeted. Victims who are children or college students often do not learn of the fraud until years later.

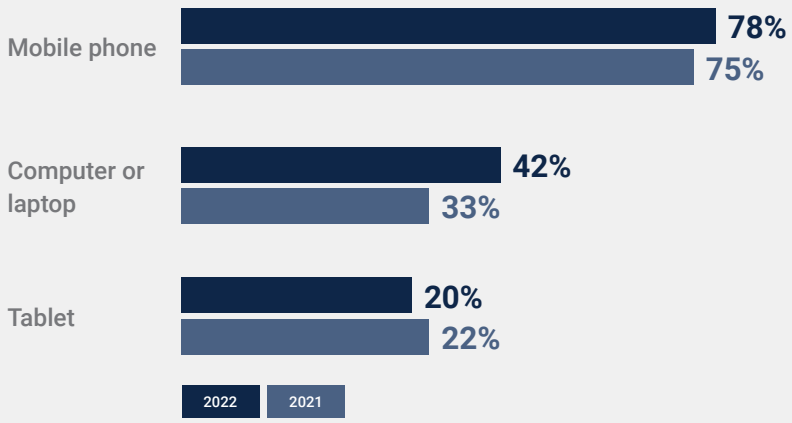
Given how consumers view the use of their personal data, how companies gather and process consumer data and the lengths they go to protect an individual's privacy, can become a point of differentiation and even a competitive business advantage.

*https://www.investopedia.com/terms/s/synthetic-identity-theft.asp
**https://risk.lexisnexis.com/insights-resources/article/synthetic-identity-fraud#:~:text=A%20synthetic%20identity%20is%20a,personally%20identifiable%20information%20(PII)

Going Increasingly Digital: Mobile is Not All that Matters

For businesses to earn consumers' trust, they must be good stewards of personal data, while providing secure and convenient interactions across all touchpoints. At the same time, businesses need to be aware of how consumers choose to interact with them. In this respect, mobile is winning. **78%** reported using a mobile device to create a new online account. Additionally, our research estimates that 151 million Americans used their mobile phone to take a picture of their identity document in 2021, that's up from 144 million in 2020.

> Which of the following did you primarily use when signing up for your new online account(s)?



While mobile accounts for the lion's share of onboarding activity, businesses still need to consider the preferences of their wider customer base. Case in point, the percentage of users who created an account online from a desktop or laptop computer rose from **33%** in 2021 to **42%** the following year.

It's also worth considering those who start on one device and may finish on the other—reaffirming the importance and convenience of cross-device workflows for all demographics. Therefore, knowing your audience is critical to knowing how to optimize your customer experience. Businesses should prioritize mobile, but they also need to ensure they create a seamless experience across all devices and channels. When the goal is to win and retain customers, it is not good enough to focus on a single aspect of the consumer experience or a single demographic. Businesses must also consider how they want to interact with consumers who do not own smartphones or have access to online services, as is the case for many underbanked and unbanked consumers. Businesses that figure out how to best support every customer, regardless of their age, their circumstances or their preferred means of interaction, will further differentiate themselves from competitors.

CONCLUSION

Delivering it All to Win Over Consumers

There is a gap between what a sophisticated business knows about identity verification and what the average consumer thinks they know. A business cannot reasonably expect the consumer to have access to advanced fraud tools or knowledge of evolving fraud schemes. Consequently, businesses are in a unique position to protect the consumer and build trust, all while preventing fraud from entering their enterprise. And this is imperative as we found that more than **70%** of consumers surveyed are considering signing up for or switching financial service providers. By taking this year's findings into account, businesses can win consumers over in an increasingly competitive marketplace by being better prepared to strike a balance between convenience and security.

This balance can be achieved by employing automated, multi-layered identity verification technology that streamlines workflows and applies friction only when needed. First impressions are important—every new customer's journey begins at the time of new account opening. To win the fight for digital consumers, businesses must ensure they provide secure onboarding workflows across different devices. If a consumer has a poor experience at one touchpoint, that affects their trust in the entire organization. Consumers aren't afraid to leave an untrustworthy, unsecure or difficult onboarding experience for one that's easier and safer.

Businesses are continuously challenged by consumers to exceed expectations for interactions—anytime, anywhere—that are as secure as they are helpful, relevant and personalized. With modern identity verification technology, businesses can meet these challenges head-on. Consumers want it all. And the good news is, you can deliver.

IDology, a GBG company, is transforming identity verification and fraud deterrence for businesses worldwide with innovative, multi-layered solutions and the data control, precision and transparency needed to build trust in a digital world. Through a combination of dedicated fraud experts and artificial intelligence, IDology leverages thousands of physical and digital data sources to deliver the industry's most accurate locate results.

Since 2003, IDology has been helping businesses stay ahead of shifting fraud trends and empowering them to build trust, deter fraud and maintain compliance for long-term revenue growth. Many of the largest technology and financial services companies in the world rely on IDology's innovative multi-channel identity verification technology, consortium network and diverse team of dedicated fraud experts.

info@IDology.com