



Authenticating Identities In The Digital Economy a PYMNTS and Mitek collaboration, reveals how consumers assess and prioritize convenience and security when using digital accounts. The report is based on a census-balanced survey of 2,255 United States consumers and examines their preferences for digital account access as well as which factors influence their views on authentication methods.

Authenticating Identities In The Digital Economy

PYMNTS.com | Mitek

December 2021

Authenticating Identities In The Digital Economy

TABLE OF CONTENTS

Introduction	04
Key Findings	06
Conclusion24
Methodology.....	.25

PYMNTS.com | Mitek

Authenticating Identities In The Digital Economy was produced in collaboration with Mitek, and PYMNTS is grateful for the company’s support and insight. [PYMNTS.com](https://www.pymnts.com) retains full editorial control over the following findings, methodology and data analysis.

Introduction

MOST DIGITAL ACCOUNT OWNERS ARE **OPEN** TO MODERN AUTHENTICATION METHODS.

The world's connected economy, which is comprised of eCommerce-enabled businesses and services, is based on "one-click" convenience that offers consumers the ability to manage their most sensitive data and transactions simply with credentials stored on devices or websites. While checking the "keep me logged in" box is simple for users, the ability to make seamless transitions from site to site across multiple devices often comes at a price. Traditional login methods, such as stored usernames and passwords, have become easier for cybercriminals to compromise, as billions of active passwords are available for sale on the dark web and artificial intelligence-driven bots launch waves of brute-force attacks on websites with increasing frequency.¹ This seems to present an unpalatable choice for consumers: convenience or security?

A new PYMNTS survey finds that most consumers prefer to use either stored credentials or basic username and password sign-ins to access their digital accounts. At the same time, they identify having too many passwords and accounts as their top digital account pain points. The affinity for traditional login methods appears to be generational: older consumers are more likely to use and prefer username and password logins, while younger individuals are more likely to prefer immediate access to accounts without a traditional login.

Despite individual differences in how consumers view identity verification, our research shows that most digital account users are open to shifting to modern authentication methods that offer a balance between convenience and security.

The ability to strike that balance — and deliver on the promise of secure, frictionless logins — presents an enormous market opportunity for technology companies. Our research found that more than three-quarters of consumers would like to use two-step authentication, such as receiving a confirmation code on a secondary device, at least periodically to ensure account security. In addition, a majority of our survey respondents agree that biometric logins are more secure and trustworthy than other methods. That means consumers are more than willing to try modern identity authentication tools, as they believe that these modern options are more secure than traditional methods such as usernames and passwords.

We also find that most American consumers see security and convenience as a prerequisite for trusting a business, brand

or website. The overwhelming majority of survey respondents want seamless login experiences (72%) and to use their preferred identity authentication method (73%).

In Authenticating Identities In The Digital Economy, a PYMNTS and Mitek collaboration, we examine why most Americans are not only open to modern methods of identity verification but also ready to trust newer technologies with their most sensitive data. Our findings were drawn from a census-balanced survey of 2,255 United States consumers conducted between Oct. 14 and Oct. 20. The survey asked consumers about their preferences for digital account access and the factors that influence their views on authentication methods.

This is what we learned.

¹ With 80% of Data Breaches Involving Passwords, Their Retirement Cannot Happen Soon Enough. PYMNTS.com. 2021. <https://www.pymnts.com/news/security-and-risk/2021/80-percent-data-breaches-involve-passwords-retirement-cannot-happen-soon-enough/>. Accessed December 2021.

Digital trust and fraud concerns

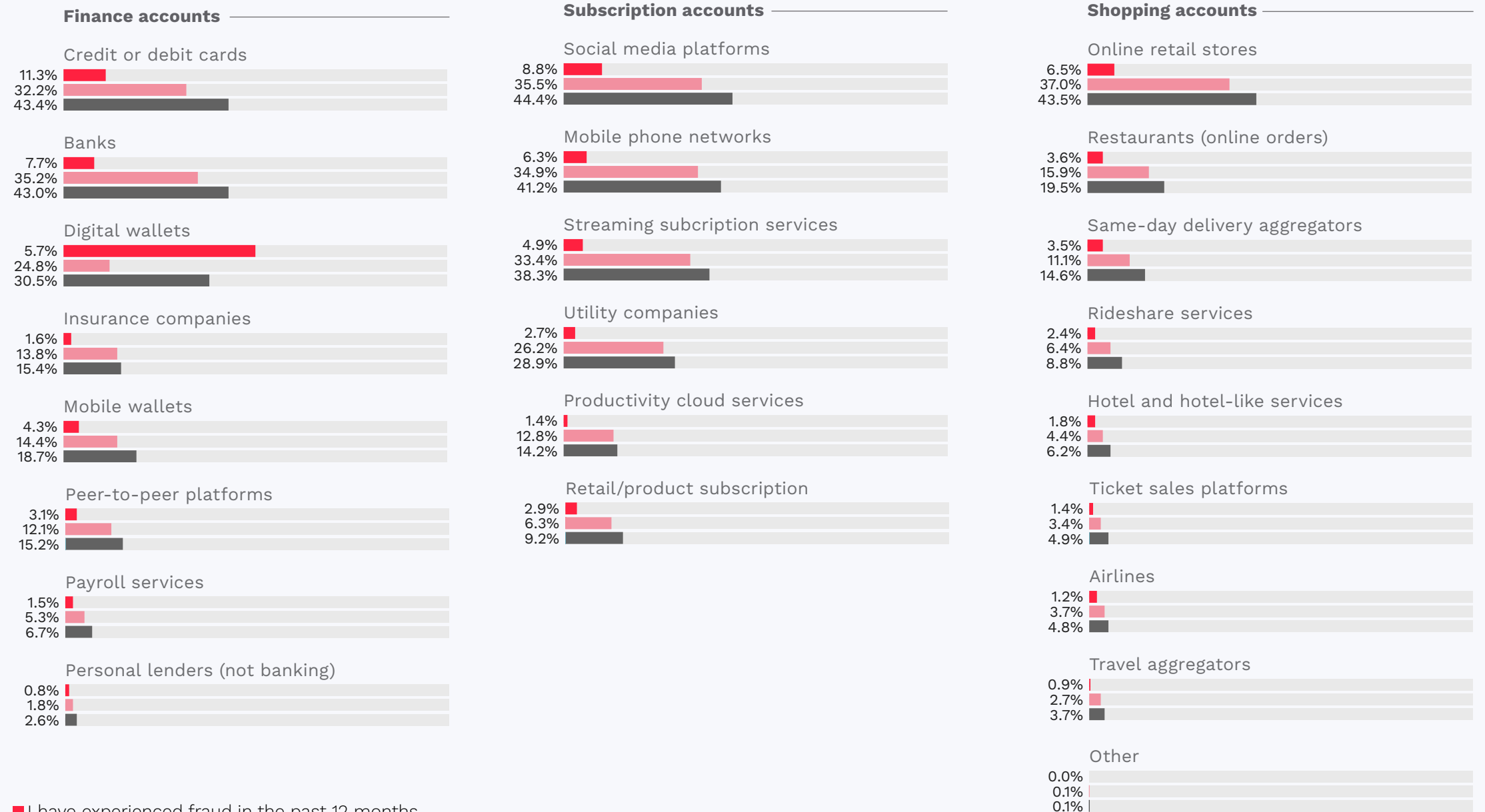
Credit and debit card users are experiencing significant levels of fraud.

Just over 10% of consumers reported an incident of fraud in connection with their digital debit and credit card accounts. Customers in larger shares also reported experiencing fraud attacks through **social media (8.8%), banks (7.7%) and online retail stores (6.5%)**. While the overall percentages of affected consumers may seem low, they should be taken in context: The Federal Trade Commission reported a 45% increase in fraud attacks between 2019 and 2020.² This meaningful increase in data compromise and the ongoing high rate of fraud experienced by credit and debit card users underscores the vulnerability of consumers' data as well as the need for alternative processes.

FIGURE 1:

Digital account users' experiences with fraud in the last 12 months

Share of respondents who use select digital account types, by experience with fraud over the last 12 months



■ I have experienced fraud in the past 12 months
 ■ I have not experienced fraud in the past 12 months
 ■ Total

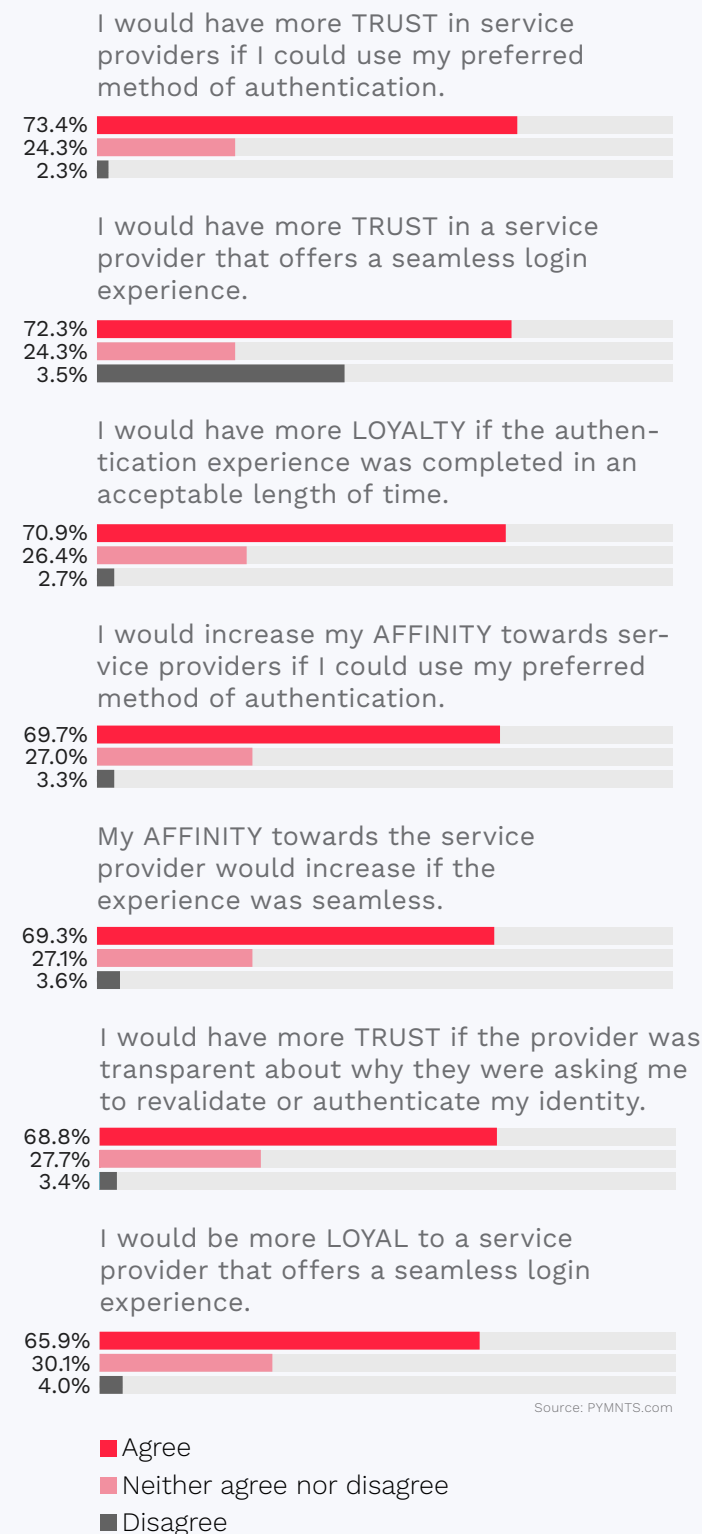
² Author unknown. Consumer Sentinel Network Data Book 2020. The Federal Trade Commission. 2021. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf. Accessed December 2021.

Nearly three-quarters of digital account users say the ability to use their preferred authentication method online and enjoy a seamless login experience boosts their trust in a service provider.

Our research finds that many digital account holders want to choose their login method: 73% of digital account users agree that being able to choose their preferred authentication method will increase their trust with a service provider, while 70% say that this will boost their affinity toward a merchant.

Consumers also want to understand how their data is handled. We found that 69% of survey respondents trust service providers more when the providers are transparent about reasons for asking users to revalidate or reauthenticate their identities. We also learned that seamless login experiences are similarly impactful, as 72% of digital account users say that seamless logins will increase their trust in a service provider, while 69% and 66% that this will boost their affinity and loyalty, respectively.

FIGURE 2:
Trust, affinity and loyalty among respondents
Share of digital account users who agree with select statements



72%

SHARE OF DIGITAL ACCOUNT USERS WHO SAY THAT SEAMLESS LOGINS WILL INCREASE THEIR TRUST IN A SERVICE PROVIDER

Authentication preferences

Despite a recent rise in fraud, less than 10% of consumers access secure biometric authentication methods.

Consumers care deeply about login experiences, but few are using fast, secure, biometric login options. Our research finds that consumers' stated preferences for logging into digital accounts were closely tied to survey respondents' ages. Older users are more likely to prefer username and password authentication, and the senior and baby boomer demographic is the most likely of all groups to choose this method.

By contrast, Generation Z and millennial users show the least interest in using manual authentication on both mobile apps (12% for Generation Z and 19% for millennials) and web browsers (25% for both). Part of the reason for the low use of biometric methods among older consumers may be poor familiarity with the technology. Millennial and Generation Z consumers are digital natives and have spent their lives online, using one-click or biometric methods to unlock their phones, log in to social

media accounts or perform a Google search. The perception among consumers unfamiliar with the technology that using biometrics requires conquering a learning curve or doing something "extra" may be a factor hindering adoption as well.

32%

SHARE OF DIGITAL ACCOUNT USERS ACCESSING ACCOUNTS FROM BROWSERS FOR WHOM **USERNAME AND PASSWORD COMBINATIONS** IS THEIR MOST PREFERRED AUTHENTICATION METHOD

FIGURE 3:






Authentication method preferences

Share of digital account users who prefer select authentication methods, by way of accessing digital accounts








TABLE 1:
Preferred authentication method, by generation

1A: Share of digital account users who prefer select authentication methods, by generation — mobile app logins

	 Generation Z	 Millennials	 Bridge millennials	 Generation X	 Baby boomers and seniors
Username and password	11.8%	18.6%	20.9%	24.9%	31.8%
PIN	9.8%	9.4%	10.4%	11.0%	9.8%
Fingerprint scan	7.3%	9.3%	11.4%	11.6%	6.3%
Face scan	11.7%	9.5%	9.6%	9.2%	4.6%
Two-step authentication method	11.6%	4.8%	5.1%	8.4%	9.8%
Mobile device code	12.0%	8.2%	8.9%	6.6%	2.3%
Personal questions with pre-specified answers	2.0%	2.0%	1.5%	1.3%	2.2%
Knowledge-based questions	2.8%	1.7%	0.7%	0.7%	1.0%
Voice scan	1.5%	1.1%	0.1%	0.0%	0.4%
Identity documents, such as passports or driver's licenses	0.0%	1.1%	1.0%	0.5%	0.0%
Other	0.6%	0.2%	0.3%	0.7%	4.9%
No need to log in or obtain immediate access with stored passwords	29.0%	34.1%	30.0%	25.2%	26.8%
Two-step authentication method					
Password and code	1.4%	1.3%	1.7%	4.8%	8.7%
Face scan and code	6.1%	1.3%	1.4%	1.3%	0.5%
Fingerprint scan and code	2.0%	1.6%	1.2%	1.6%	0.6%
Voice scan and code	2.1%	0.6%	0.8%	0.7%	0.0%

Source: PYMNTS.com

1B: Share of digital account users who prefer select authentication methods, by generation — web browser logins

	 Generation Z	 Millennials	 Bridge millennials	 Generation X	 Baby boomers and seniors
Username and password	24.7%	25.1%	28.2%	30.4%	44.5%
PIN	10.7%	10.0%	10.6%	11.9%	7.2%
Fingerprint scan	6.7%	8.3%	9.9%	6.1%	3.4%
Face scan	3.3%	6.1%	6.3%	7.9%	2.5%
Two-step authentication method	11.3%	8.4%	7.2%	8.3%	10.3%
Mobile device code	N/A	N/A	N/A	N/A	N/A
Personal questions with pre-specified answers	3.1%	3.5%	3.0%	2.8%	2.0%
Knowledge-based questions	2.0%	0.7%	0.6%	0.9%	0.7%
Voice scan	1.4%	1.1%	0.7%	0.0%	0.3%
Identity documents, such as passports or driver's licenses	0.7%	0.8%	0.6%	0.2%	0.0%
Other	0.4%	0.1%	0.2%	0.6%	0.9%
No need to log in or obtain immediate access with stored passwords	35.8%	35.9%	32.8%	30.9%	28.2%
Two-step authentication method					
Password and code	6.6%	4.2%	4.1%	5.1%	8.4%
Face scan and code	3.1%	1.2%	0.8%	0.9%	0.7%
Fingerprint scan and code	1.2%	1.8%	1.2%	1.5%	1.1%
Voice scan and code	0.4%	1.2%	1.0%	0.8%	0.1%

Source: PYMNTS.com

Nice and easy

Consumers see biometric methods as easy to use, and 44 percent of digital account users cited ease of use as their top reason for preferring an authentication method.

PYMNTS' research reveals that consumers view ease of use as the top reason why they prefer particular authentication methods, including biometrics. Ease of use is key to consumer preference among all users, including those who prefer PINs and biometric authentication methods for both mobile app and browser-based log-ins.

Only three authentication methods exhibit substantially different patterns: two-step authentication, mobile device code authentication (mobile app users only) and personal questions with pre-specified answers (browser users only). Smaller shares of respondents who favor these methods point to ease of use as the top reason for their preference, and larger portions identify account security and preventing theft as their top motivation.

PYMNTS' research finds that biometric authentication methods earn appreciation for their ease of use. Slightly more than half of mobile app users (51%) and browser users (52%) report that ease of use was the most important reason why they prefer fingerprint scans. Face scan authentication received similar accolades: 49% of both app users and browser users say ease of use was the most important reason why they select face scan authentication. Generation Z mobile app users are more than twice as likely as baby boomers and seniors to say they prefer face scan authentication (12% versus 5%).

51%

PORTION OF MOBILE APP USERS WHO REPORT THAT EASE OF USE WAS THE **MOST IMPORTANT** REASON WHY THEY PREFER **FINGERPRINT SCANS**

TABLE 2:
Most important reasons for authentication preferences

2A: Share of respondents who access digital accounts using mobile apps and select a given reason as their top choice, by method

	Sample	Username and password	Having my app/ browser automatically enter the password	Entering a PIN	Fingerprint scan	Face scan	Two-step authentication method	Mobile device code
It is easy to use.	44.2%	40.0%	46.0%	50.5%	50.9%	48.9%	27.7%	30.4%
It is a faster way to log in to my accounts.	15.9%	14.3%	19.7%	12.0%	13.9%	19.6%	11.7%	9.9%
I receive better data protection.	11.5%	16.3%	6.9%	12.8%	15.6%	8.6%	18.4%	6.5%
I am less likely to experience theft of my money or assets.	11.2%	7.7%	6.4%	8.7%	9.6%	10.7%	30.1%	29.9%
It is easier for me to remember how to access the account.	11.1%	15.5%	14.6%	12.6%	4.7%	8.8%	6.2%	11.2%
It makes it easier to use the digital account more frequently.	5.1%	5.2%	3.8%	3.3%	4.6%	3.50%	5.1%	12.1%
Other	0.9%	0.9%	2.5%	0.0%	0.7	0.0%	0.8%	0.0%

Source: PYMNTS.com

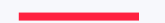
Most important reasons for authentication preferences

2B: Share of respondents who access digital accounts using internet browsers and select a given reason as their top choice, by method

	Sample	Username and password	Having my app/ browser automatically enter the password	Entering a PIN	Fingerprint scan	Face scan	Two-step authentication method	Personal questions with pre-specified answers
It is easy to use.	46.4%	45.1%	48.1%	47.0%	51.9%	48.9%	29.6%	36.3%
It is easier for me to remember how to access the account.	15.2%	16.6%	16.5%	20.6%	3.0%	8.8%	13.7%	15.2%
I receive better data protection.	11.5%	11.6%	7.0%	10.3%	11.1%	17.3%	24.5%	14.2%
It is a faster way to log in to my accounts.	11.4%	9.4%	17.1%	7.1%	18.6%	18.1%	4.5%	9.7%
I am less likely to experience theft of my money or assets.	9.6%	10.6%	4.8%	9.4%	7.6%	3.7%	23.7%	17.7%
It makes it easier to use the digital account more frequently.	5.2%	6.0%	6.1%	5.0	7.1%	3.2%	2.5%	6.9%
Other	0.6%	0.7%	0.4%	0.5%	0.7	0.0%	1.5%	0.0%

Source: PYMNTS.com

69%
SHARE OF **BABY BOOMERS AND SENIORS** WILLING TO USE TWO-FACTOR AUTHENTICATION



Why do so many consumers value easy logins above all else? One driving factor: They have too many passwords and accounts to deal with. Nearly half of all digital account users identified having too many passwords as their top pain point for accessing their accounts (46%), followed by the sheer number of accounts themselves (38%) and inability to use the same passwords across accounts due to different rules (33%).

Smaller but still sizable shares of digital account users also point to similar headaches, including being unable to remember all the ways they access accounts (19%) and the time it takes to create new passwords (19%). These trends vary relatively little across generations: having too many passwords, having too many accounts and being unable to reuse the same password are the top three pain points for consumers, regardless of age group.

Despite lower usage rates for two-step authentication methods, the vast majority of consumers of all ages are open to their use periodically. More than one-third of consumers would like to use two-step authentication when they access their accounts from new devices, while 27% would prefer to use it for each login and

15% would do so once a month. We found that 83% of millennials and 81% of bridge millennials are willing to use two-factor authentication, while 69% of baby boomers and seniors stated the same.

36%

SHARE OF DIGITAL ACCOUNT USERS WHO PREFER TWO-STEP AUTHENTICATION WHEN LOGGING IN FROM A **NEW DEVICE**

FIGURE 4:
Preferred frequency of two-step authentication use
Share of digital account users who prefer to utilize two-step authentication, by frequency

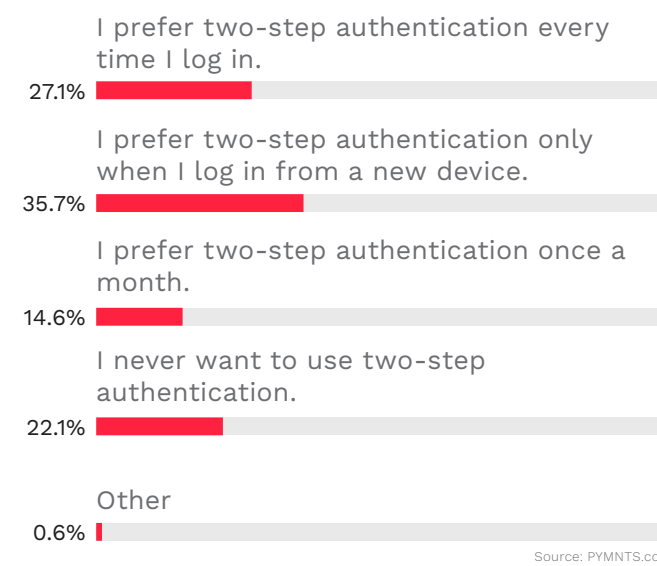


TABLE 3:
Preferred frequency of two-step authentication use by generation
Share of digital account users who prefer to utilize two-step authentication, by frequency and generation

	Generation Z	Millennials	Bridge millennials	Generation X	Baby boomers and seniors
I prefer two-step authentication every time I log in.	20.4%	29.1%	30.3%	29.0%	25.8%
I prefer two-step authentication only when I log in from a new device.	40.7%	36.2%	34.4%	35.4%	33.1%
I prefer two-step authentication once a month.	20.3%	17.4%	16.4%	13.1%	10.5%
I never want to use two-step authentication.	18.1%	16.6%	17.9%	21.5%	30.1%
Other	0.5%	0.6%	0.9%	0.9%	0.5%

Source: PYMNTS.com

Four key biometric authentication terms to know

Biometric user authentication looks at much more than entered data to authenticate a user. It examines biological attributes, such as facial recognition or the live sound of someone's voice, as well as other data to whitelist a user. Biometric logins offer stronger security than traditional stored username and password identity verification because they are harder to spoof and normally require a user to interact with a verification method in real time. They often use behavioral biometrics to determine the legitimacy of the data entered, rather than simply comparing a username and password to information stored in a database.

Multimodal authentication

Multimodal authentication refers to the use of multiple biometric markers to authenticate a user. For example, a mobile application can use voice and facial recognition data to verify users' identities securely.

Step-up authentication

Step-up authentication is a way to reduce friction by requiring an additional authentication factor only when the risk level increases. This may occur when the user is attempting to complete a transaction that requires strong authentication, such as transferring funds over a certain limit, changing the mailing address on a bank account or requesting access to certain resources.

Active and passive liveness

Active liveness detection relies on the user's movements in response to challenges such as nodding, blinking, smiling or correctly positioning one's face in a frame. While the technology can be effective at detecting a spoof, it introduces friction into a verification or authentication process. Passive liveness detection is fundamentally different in that it requires no action by the user, providing advantages such as a faster process, less confusion for the user and lower abandonment rates.

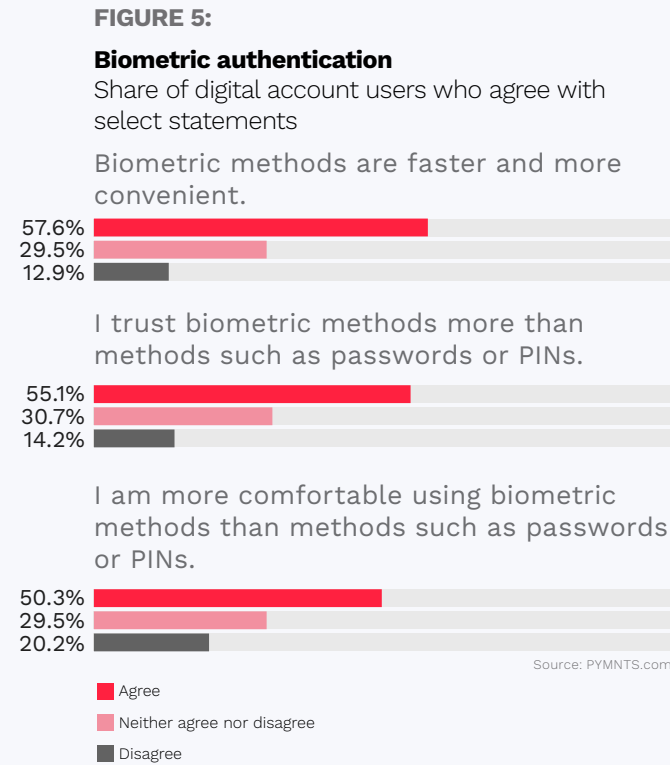
Liveness detection

When using biometrics for identity verification or authentication, liveness detection ensures the presence of a live user in front of the capture device, such as a camera, microphone or fingerprint reader. Liveness detection is important because biometric tools only answer the question "is this the right user?" In other words, biometrics alone cannot distinguish between a live user and a spoof, such as a photo, video or recording of the user.

Seamlessly building trust

Our data shows that 58% of consumers believe that biometric authentication methods are faster and more convenient than alternatives and 55% of consumers trust them more than methods.

Approximately half of respondents feel more comfortable with biometric authentication than with other login methods. These results highlight that many consumers recognize the advantages of biometric logins and are very willing to switch to authentication technologies such as fingerprint scans and facial identification, even though relatively few currently identify these as their most preferred methods.



55%

PORTION OF CONSUMERS WHO TRUST BIOMETRIC METHODS MORE THAN PASSWORDS AND PINs

Conclusion

Nearly all U.S. consumers use at least one type of digital account to access entertainment, shopping, their finances and other online services. They are doing so much more frequently now than they did 12 months ago, and this trend of digital growth will likely continue to accelerate. Identity verification is a core part of digital account access, and it is one that can either create headaches or enrich the user experience. Most digital account users prefer authentication methods they associate with ease, and they cite having too many passwords and accounts to remember as key pain points. Relatively few digital account users say that they currently prefer two-step or biometric authentication, yet our research shows that the majority recognize these methods' benefits. Our research indicates that older consumers are most likely to show a preference for traditional username and password authentication, with millennials and Generation Z showing the greatest interest in alternatives. Businesses should strive for account holders to enjoy seamless login experiences and be empowered to use the authentication methods of their choice. Doing so will strengthen the trust, affinity and loyalty that users feel toward service providers.

Methodology

Authenticating Identities In The Digital Economy, a PYMNTS and Mitek collaboration, is based on census-balanced surveys of 2,255 U.S. consumers conducted between Oct. 14 and Oct. 20 as well as an analysis of other economic data. The sample was constructed to match the U.S. adult population in key demographic characteristics. Respondents averaged 48 years of age, 52% were female, and 32% held college degrees. The sample also covered different income brackets: 36% of respondents earned over \$100,000 a year, while 31% have incomes of \$50,000 to \$100,000 and 33% earn less than \$50,000.

**Authenticating
Identities** In The
Digital Economy

About

DISCLAIMER

PYMNTS.com [PYMNTS.com](#) is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Mitek (NASDAQ: MITK) is a global leader in mobile capture and digital identity verification solutions built on the latest advancements in AI and machine learning. Mitek’s identity verification solutions enable an enterprise to verify a user’s identity during a digital transaction, which assists financial institutions, payments companies and other businesses operating in highly regulated markets in mitigating financial risk and meeting regulatory requirements while increasing revenue from digital channels. Mitek also reduces the friction in the users’ experience with advanced data prefill and automation of the onboarding process. Mitek’s innovative solutions are embedded into the apps of more than 6,100 organizations and used by more than 80 million consumers for mobile check deposit, new account opening and more.

For more information, visit us at www.miteksystems.com

Authenticating Identities In The Digital Economy may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED “AS IS” AND ON AN “AS AVAILABLE” BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.