

The Future Of Authentication In Financial Services, a PYMNTS and Entersekt collaboration, examines authentication's role in financial services and illustrates how financial institutions can provide consumers with trusted and integrated banking experiences across multiple environments.

PYMNTS.com

Entersekt

THE FUTURE OF AUTHENTICATION IN FINANCIAL SERVICES

Finding The Balance Between
Security And Convenience

THE FUTURE OF AUTHENTICATION IN FINANCIAL SERVICES

TABLE OF CONTENTS

Introduction	04
The importance of protecting personal data	08
What makes for trusted consumer experiences	12
The security mandate	16
A secure yet simple solution	20
Conclusion	24
Methodology	25

PYMNTS.com



The Future Of Authentication In Financial Services was produced in collaboration with Entersekt, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

INTRODUCTION

As life becomes more digitally connected, consumers increasingly expect that all online transactions will be highly secure, simple and convenient. This standard is especially strong among consumers who use digital banking to access their accounts across multiple digital platforms, including mobile apps and mobile- and desktop-based browsers.

More than three-quarters of consumers who regularly use digital channels to interact with their financial services providers believe that their personal data is valuable to at least one entity other than their financial institutions (FIs) and that the security of their personal data when transacting online is extremely important.

Our research finds that feeling secure while transacting online is a key driver of consumers' trust in financial services providers, as is a consistent user experience across different platforms. When push comes to shove, however, most consumers value security over ease of use and convenience. Providers may not need to choose one or the other, however: By moving away from passwords and toward stronger authentication methods, financial

services providers can support secure logins and transactions while also simplifying the consumer experience.

The Future Of Authentication In Financial Services Playbook: Finding The Balance Between Security And Convenience, a PYMNTS and Enterspekt collaboration, examines consumers' expectations that their financial experiences will be highly secure across a range of digital channels and devices.

MOST CONSUMERS
PREFER **SECURITY**
OVER CONVENIENCE.

We surveyed 2,719 consumers from Sept. 10, 2021, through Sept. 27, 2021, to learn more about how these expectations vary across different type of accounts and how balancing convenience and security impacts consumers' trust in their financial providers.

This is what we learned.

01

MORE THAN HALF OF CONSUMERS CONSIDER DATA SECURITY “EXTREMELY” IMPORTANT WHEN SHARING PERSONAL DATA ONLINE. MOST CONSUMERS SAY THEIR PRIVATE DATA IS VALUABLE TO ENTITIES OTHER THAN THEIR FIs.

The security of personal data when transacting online is “extremely” important for 52% of respondents, while another 28% find it “very” important. Nearly four-fifths of consumers say their personal data is valuable to at least one entity other than their FIs, with 24% saying their personal data is valuable to all types of entities.

02

SECURITY AND A GOOD USER EXPERIENCE ARE HIGHLY INFLUENTIAL IN BUILDING CONSUMER TRUST IN FINANCIAL PROVIDERS. CONSISTENCY ACROSS DIFFERENT PLATFORMS IS ALSO CRITICAL TO MOST CONSUMERS’ TRUST.

Security is “highly” important for 83% of respondents, and a good user experience is “highly” important for 80%. We also find that 53% of consumers say consistent experiences across different platforms have a “very” or “extremely” big impact on their trust in FIs. This share is higher among consumers who access their accounts mostly using mobile apps or through multiple environments, at 60% and 58%, respectively.

03

FOUR OUT OF 10 CONSUMERS ARE “VERY” OR “EXTREMELY” CONCERNED ABOUT THE SECURITY OF THEIR PRIVATE DATA. MOST CONSUMERS PREFER SECURITY OVER CONVENIENCE.

PYMNTS’ data finds that 38% of consumers are “very” or “extremely” concerned about data security when using their digital financial service accounts. Respondents with online-only bank accounts are most likely to be concerned, at 47%, while the smallest share of concern is held by those with online accounts at traditional banks: 33%. Consequently, 68% of respondents choose security over convenience, and 75% of online brokerage firm account holders choose security over convenience, leading the pack.

04

SIX OUT OF 10 CONSUMERS ARE WILLING TO LOG IN TO THEIR ACCOUNTS WITH ALTERNATIVE AUTHENTICATION METHODS. THIS SHARE RISES TO 73% FOR USERS WHO LEVERAGE MULTIPLE DEVICES TO ACCESS THEIR ACCOUNTS.

Sixty-one percent of consumers are willing to log in to their accounts with alternative authentication methods, and 60% of those who use mobile apps, mobile browsers and computer browsers say they would be “very” comfortable logging in using methods other than login IDs and passwords. Just under half of these users believe passwords will eventually be phased out as an authentication method.



THE IMPORTANCE OF PROTECTING PERSONAL DATA

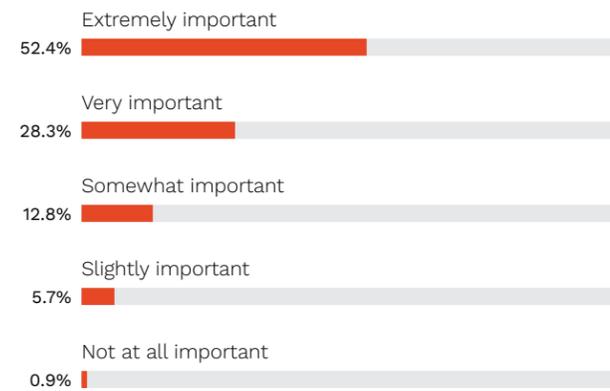
THE FUTURE OF AUTHENTICATION IN FINANCIAL SERVICES

PYMNTS.com



FIGURE 1A:
Perceptions around sharing personal data online

Share of consumers who agree data security is important when sharing personal data

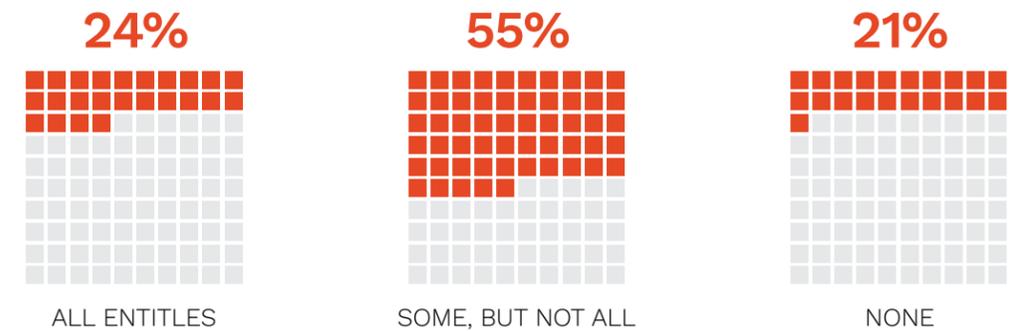


N = 2,719: Digital financial account owners
Source: PYMNTS | Entersekt
The Future Of Authentication In Financial Services

PYMNTS’ research finds that close to 80% of consumers believe that their private data is valuable to entities other than their financial services providers. It is no surprise, then, that a similar share of consumers consider data security to be “very” or “extremely” important when sharing this personal data online. For 52% of respondents, the security of their personal data is “extremely” important when sharing it online, and 28% find it “very” important.

FIGURE 1B:
Perceptions around sharing personal data online

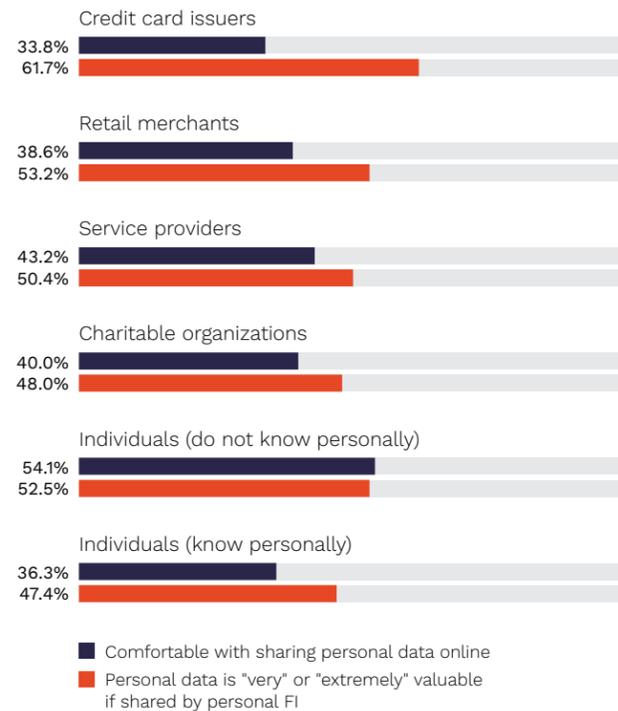
Number of entities that consumers think have a strong interest in their personal data



N = 2,719: Digital financial account owners
Source: PYMNTS | Entersekt
The Future Of Authentication In Financial Services

FIGURE 1C:
Perceptions around sharing personal data online

Share of consumers who agree with select statements about sharing personal data with different entities

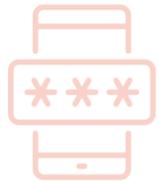


N = 2,719: Digital financial account owners
 Source: PYMNTS | Enterspekt
 The Future Of Authentication In Financial Services

Consumers sense that many desire their information, though 79% of account holders believe their data is coveted by at least one entity other than their FIs, with 24% believing that all types of third-party entities want their data. The entities that online financial service account holders say want their data include individuals they know personally, individuals they do not know personally, charitable organizations, credit card-issuing banks, retail merchants and financial services providers they do not use. Only 21% of consumers believe their data is not coveted by other entities.

Consumers are most likely to perceive their personal data as “very” or “extremely” valuable if shared with credit card companies, with 62% saying so, followed by retail merchants at 53%. Only 34% of consumers are comfortable sharing personal data online with credit card companies, and just 39% are comfortable doing so with retail merchants.





WHAT MAKES FOR TRUSTED CONSUMER EXPERIENCES

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

PYMNTS.com

 Entersekt

Though security is highly influential in consumers' trust in their financial providers, so is a good user experience. PYMNTS' research finds that trusted user experiences are highly important to consumers when accessing digital accounts via any channel. In fact, 80% of consumers believe that having a good user experience has a "very" or "extremely" big impact on their trust in their financial services providers.

One key measure that impacts the user experience is consistency, as 53% of consumers assert that having a consistent experience across different platforms — including online banking, app banking and using the institution's card for eCommerce — has a "very" or "extremely" big impact on their trust in their FIs, and an additional 31% say it has a "moderate" impact. This share increases among consumers who access their accounts mostly using mobile apps or through multiple environments, at 60% and 58%, respectively — two groups that would be expected to notice the consistency, or lack thereof, that a provider may have engineered.

Security remains important when consumers are building trust: 83% of consumers say that their financial service provider having at least one security enhancing feature has a "very" or "extremely" big impact on their trust in that provider. Moreover, 65% of consumers say that providers' emphasis on data security has the same high level of impact on their trust. Our data shows that 60% of consumers say that having information about how their transactions are secured has a "very" or "extremely" big impact on their trust, and 44% of consumers say that the ability to log in without passwords has a similarly strong impact.

FIGURE 2:

What builds trust in financial services providers

Share of consumers who cite select factors as “very” or “extremely” impactful on their trust in a financial services provider

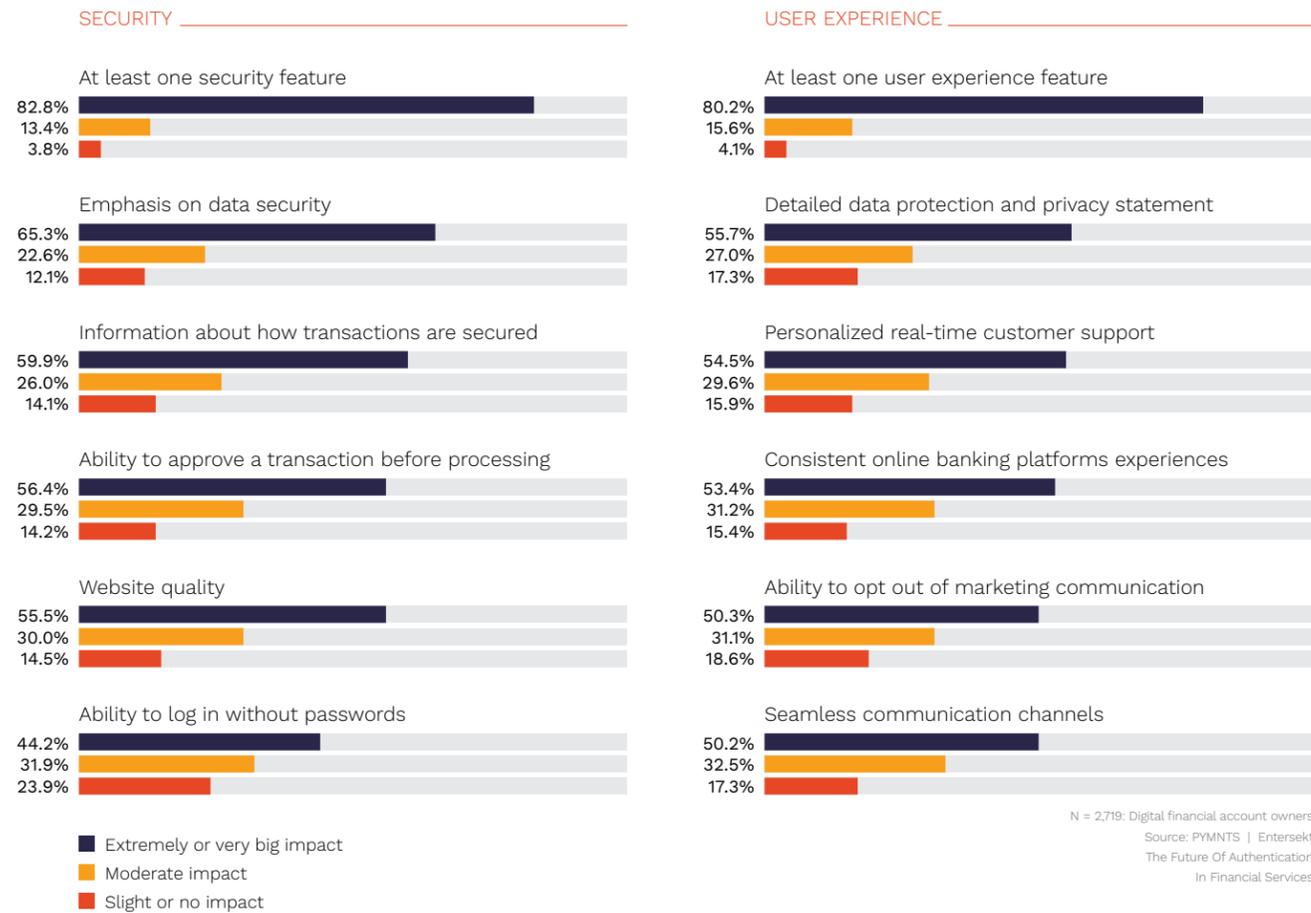
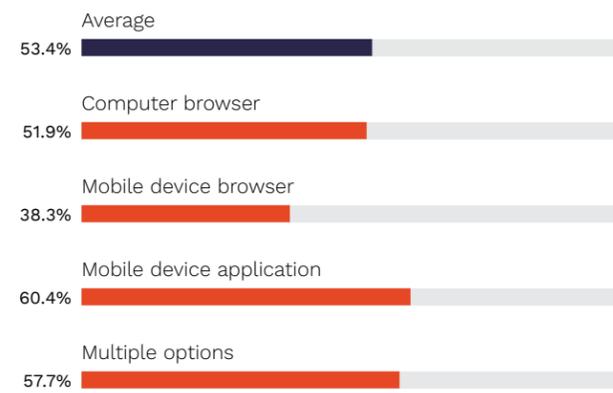


FIGURE 3:

The importance of consistency in building trust

Share of consumers who believe a consistent experience has a “very” or “extremely” big impact on their trust in their financial services providers, by channel most frequently used for account access



N = 2,719; Digital financial account owners
Source: PYMNTS | Enterspekt
The Future Of Authentication In Financial Services



Share of consumers who say that the ability to log in without passwords has a “very” or “extremely” big impact on their trust in their financial services providers





THE SECURITY MANDATE

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

PYMNTS.com

Entersekt

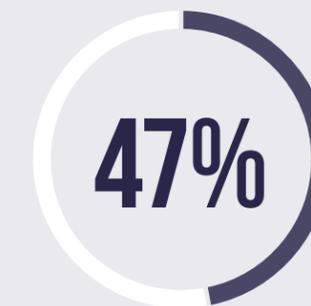
PYMNTS' data finds that 38% of consumers report being "very" or "extremely" concerned about data security when using digital financial services accounts. Online-only bank account holders are the most likely to be concerned with security at 47%, compared to just 33% of those with online accounts at traditional banks.

Consumers' concern about their personal information's security is a priority when interacting with their financial service providers online. Security outweighs the needs for

convenience and ease of use: 68% of respondents would choose security over convenience when transacting with their financial services providers, and only 24% remain neutral. This pattern holds true across all types of accounts, yet account holders value security over convenience, especially with accounts that typically provide long-term holdings or stability. Our data finds that 72% of online insurance account holders would choose security over convenience, and 75% of online brokerage firm account holders would do so as well.



Share of consumers with online accounts at traditional banks who report being "very" or "extremely" concerned about data security when using digital financial services accounts



Share of online-only bank account holders who report being "very" or "extremely" concerned about data security when using digital financial services accounts



Share of respondents who would choose security over convenience when transacting with their financial services providers

FIGURE 4A:

Consumers' concern with data security when using online financial services accounts

Share of consumers who are "very" or "extremely" concerned about data security when using online financial services accounts, by financial services provider

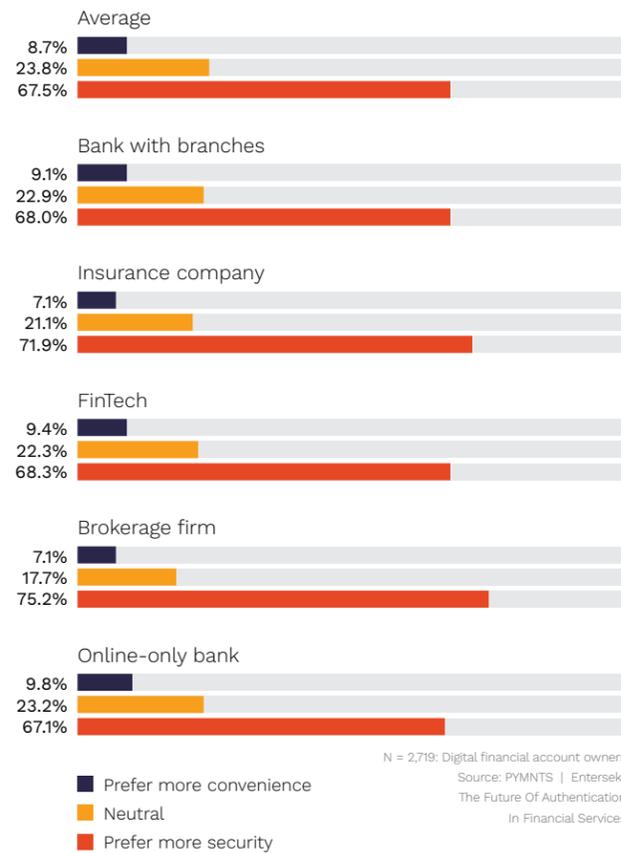


N = 2,719: Digital financial account owners
Source: PYMNTS | Enterspekt
The Future Of Authentication In Financial Services

FIGURE 4B:

Consumers' concern with data security when using online financial services accounts

Share of consumer who prefer more convenience or security, by financial services provider



N = 2,719: Digital financial account owners
Source: PYMNTS | Enterspekt
The Future Of Authentication In Financial Services

■ Prefer more convenience
■ Neutral
■ Prefer more security



Share of online brokerage firm account holders who would choose security over convenience

Consumers' concern about their personal information's security is a priority when interacting with their financial service providers online.



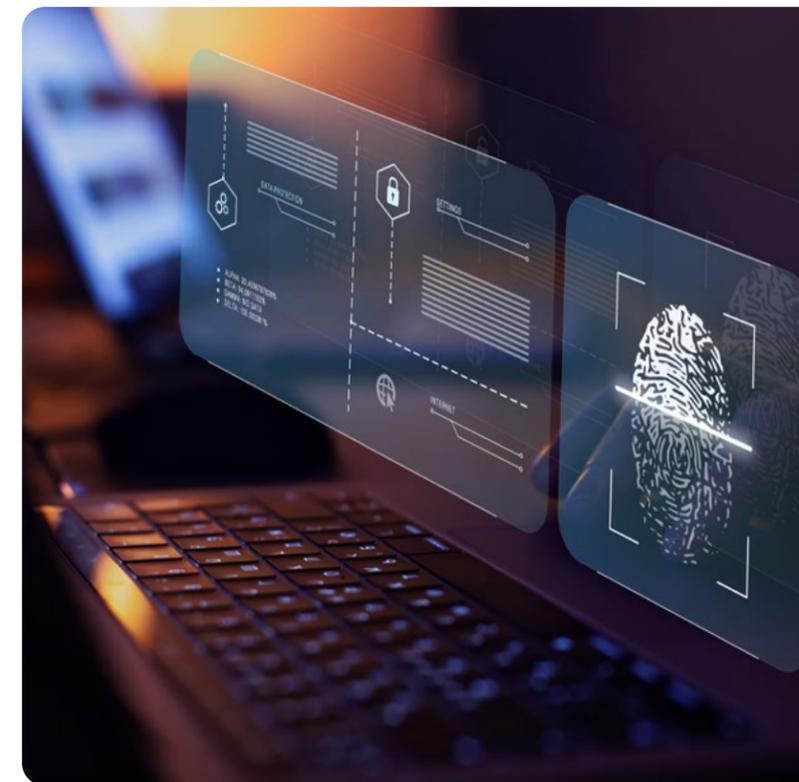
A SECURE YET SIMPLE SOLUTION

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

PYMNTS.com



Moving away from passwords to stronger biometric authentication measures is one way that financial services providers can support secure logins and transactions while simplifying the consumer experience. PYMNTS' research finds that 61% of consumers are willing to use login methods other than passwords, and consumers who mostly use mobile apps or multiple environments to access digital accounts are the most willing to do so at 68% and 73%, respectively.



Share of consumers who mostly use mobile apps to access digital accounts and are willing to use login methods other than passwords



Share of consumers who mostly use multiple environments to access digital accounts and are willing to use login methods other than passwords

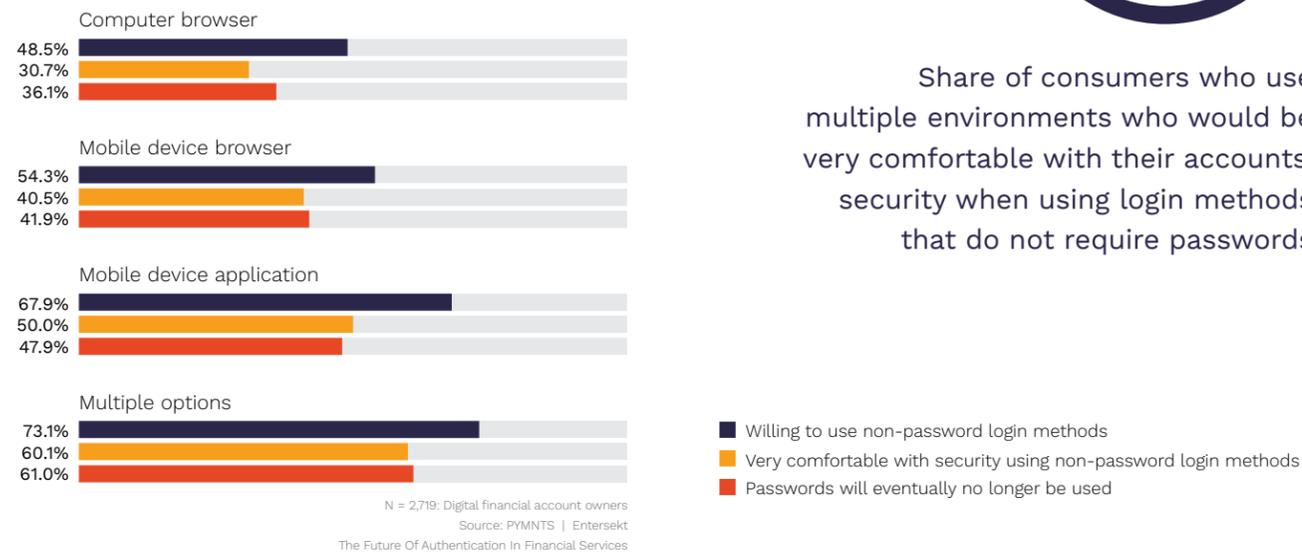
FIGURE 5A:

Consumers' comfort with logging in to accounts without passwords

Share of consumers who agree with select statements about logging into their accounts without passwords, by most frequently used device



Share of consumers who use multiple environments who would be very comfortable with their accounts' security when using login methods that do not require passwords



Consumers' growing confidence in the use of alternative authentication methods is evident. We find that 45% of respondents report they would be very comfortable with their accounts' security when using login methods that do not require passwords, and this share swells to 60% for consumers who use multiple environments. By and large, consumers are beginning to let go of passwords: 47% believe that passwords eventually will not be used at all, with consumers who use multiple environments to access accounts the most likely to agree at 61%.

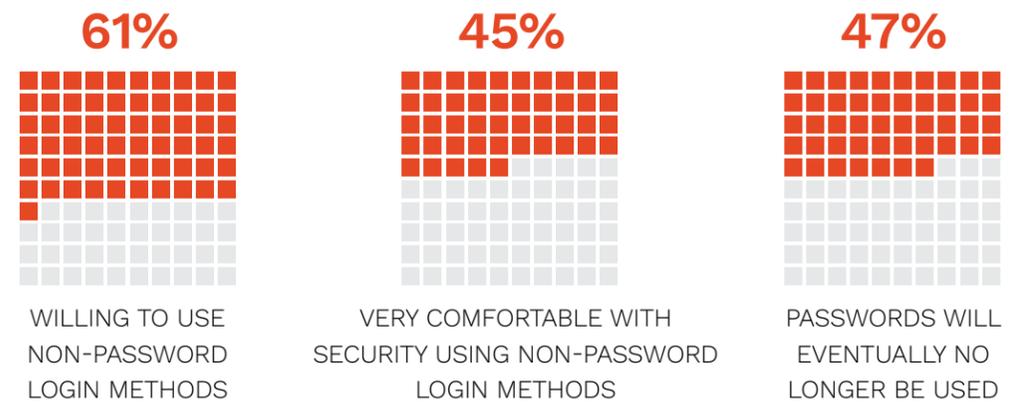
Moving away from passwords to stronger biometric authentication measures

is one way that financial services providers can support secure logins and transactions.

FIGURE 5B:

Consumers' comfort with logging in to accounts without passwords

Share of consumers who agree with select statements about logging in to their accounts without passwords



N = 2,719: Digital financial account owners
 Source: PYMNTS | Enterspekt
 The Future Of Authentication In Financial Services

CONCLUSION

As today's connected consumers move more of their interactions with their financial services providers online and complete them via computer browsers or mobile devices, they are becoming increasingly concerned with the security of their personal data and are not always comfortable with how this data is shared with other entities. Digitally savvy consumers, especially those who transact via multiple devices, also expect best-in-class experiences defined by convenience — and to get these experiences consistently across devices. The challenge for financial services providers is to find a balance between security and convenience, as both are key factors to building consumer trust. Stronger, passwordless authentication, which not only simplifies the consumer authentication experience but also supports frictionless and secure logins and transactions, is one way that financial services providers can find this balance and reinforce consumer trust.

PYMNTS.com

 Entersekt

METHODOLOGY

The Future Of Authentication In Financial Services: Finding The Balance Between Security And Convenience, a PYMNTS and Entersekt collaboration, draws from a PYMNTS survey of 5,578 American consumers who were asked about their preferences for different types of authentication when accessing their financial service accounts across various digital environments (e.g., desktop/laptop versus mobile). We removed 563 responses from our original sample due to illegibility, inaccuracies or other issues, and we eliminated another 1,018 for incompleteness. This left us with 3,997 responses, of which 2,719 were from respondents who had bank accounts, owned mobile devices and used mobile banking apps. Our analysis considered the response data from this group, and our weighted sample was then census-balanced in terms of age, education level, gender and income.

THE FUTURE OF
AUTHENTICATION
IN FINANCIAL SERVICES

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.

 **Entersekt** is a leading provider of strong device identity and customer authentication software. Financial institutions and other large enterprises in countries across the globe rely on its multipatented technology to communicate with their clients securely, protect them from fraud, and serve them convenient new experiences irrespective of the channel or device in use. They have repeatedly credited the Entersekt Secure Platform with helping to drive adoption, deepen engagement, and open opportunities for growth, all while meeting their compliance obligations with confidence. For more information, please visit www.entersekt.com or email info@entersekt.com.

The Future Of Authentication In Financial Services 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.