

PYMNTS

entersekt

Visible and Invisible Security: Perceptions in Digital Banking

March 2023 ■

Visible and Invisible Security: Perceptions in Digital Banking, a PYMNTS and Entersekt collaboration, examines consumers' authentication preferences for online financial transactions. This report is based on a census-balanced survey of 2,584 U.S. consumers conducted between Sept. 26, 2022, and Oct. 3, 2022.





Visible and Invisible Security:

Perceptions in Digital Banking

Table of Contents

| | |
|--|----|
| Introduction | 04 |
| Securing routine online financial transactions | 08 |
| Seeing is believing: Visible security and trust. | 10 |
| The security mandate: More measures, visible and invisible | 14 |
| The power of passwordless methods | 16 |
| Conclusion | 20 |
| Methodology. | 21 |

Visible and Invisible Security: Perceptions in Digital Banking was produced in collaboration with Enterspekt, and PYMNTS is grateful for the company's support and insight. [PYMNTS](#) retains full editorial control over the following findings, methodology and data analysis.

Introduction

Consumers have had to accept whatever security systems financial institutions (FIs) rolled out, but that is beginning to change. With advances in authentication technologies and growing consumer awareness of types of security measures, retail banking customers are increasingly voicing their preferences for more user-friendly and secure options for verifying their identity or making payments online.

PYMNTS' latest research found that 36% of banking customers want their FIs to offer more visible security measures — those that require a user to act, such as entering a password or using biometric authentication — for high-risk financial activities. Most consumers who want additional visible security measures believe that their assets and personal information are more secure when they see additional visible security measures in place.

Our study also shows that the long reign of passwords as the dominant online identity authentication method is ending — and biometric authentication is taking the lead. Fifty-two percent of consumers using biometrics for authentication report this method as their favorite, while just 16% of password users feel the same.

Banks must embrace this new reality by offering consumers the additional visible security measures they want and allowing them to customize their authentication experiences according to their preferences. Visible and Invisible Security: Perceptions in Digital Banking, a PYMNTS and Entersekt collaboration, examines consumers' preferences for visible and invisible online authentication methods. This report is based on a census-balanced survey of 2,584 United States consumers conducted between Sept. 26, 2022, and Oct. 3, 2022.

This is what we learned.

Consumers — especially millennials — want to be **more involved** in protecting their money and identity, even in everyday financial activities.

Twenty-seven percent of banking consumers want their FIs to provide additional visible security measures for routine digital activities, with 30% looking for added security when accessing bank accounts, 29% when sending or receiving money and 27% when making purchases. The preference for additional visible security measures is present across demographic groups, with millennials leading the pack at 37%.

Banks can **bolster consumer trust** by implementing additional visible security measures for high-risk online financial transactions.

Thirty-six percent of online banking customers want additional visible security measures for high-risk financial activities and transactions, with 38% looking for more visible security when accessing their bank accounts from a new device and 37% when making large online transactions. Nearly two-thirds of consumers believe increased visible security measures make their assets safer. Millennial, Generation Z and Generation X consumers are more likely to want additional visible security, with baby boomers and seniors the exception.

Customers of digital-only banks **crave** additional security measures for frequent digital financial activities and transactions.

Regardless of where they bank, consumers want additional visible and invisible security measures at similar rates, with one exception. Consumers who use digital-only banks demand additional invisible security measures at higher rates than those who use traditional banks. This preference, however, does not reduce their calls for additional visible security measures. When considering specific transaction types, all consumers expressed greater interest in more visible security measures. While 41% of both digital-only and traditional bank customers want additional visible security measures when accessing their bank accounts from a new device, 34% of digital-only banking customers want these measures for subsequent access, versus 31% of traditional bank customers.

Banks **should increase** their visible security offerings by implementing passwordless authentication measures that consumers prefer and trust.

The authentication landscape is quickly shifting from passwords to biometrics and multifactor authentication (MFA) methods, with 47% of consumers relying on biometrics in the past month and 52% of biometric authentication users preferring it over other methods. Consumers who prefer biometrics primarily cite convenience, ease of use and security as the top benefits, while those that favor MFA point to stronger security as its leading advantage.

Securing routine online financial transactions

Even though infrequent, high-risk digital transactions and financial activities capture the security spotlight, many consumers also want more visible options in routine contexts. We found that 47% of consumers report being less than satisfied with their FIs' current security measures for routine digital activities and transactions, and 27% said their FIs should do more.

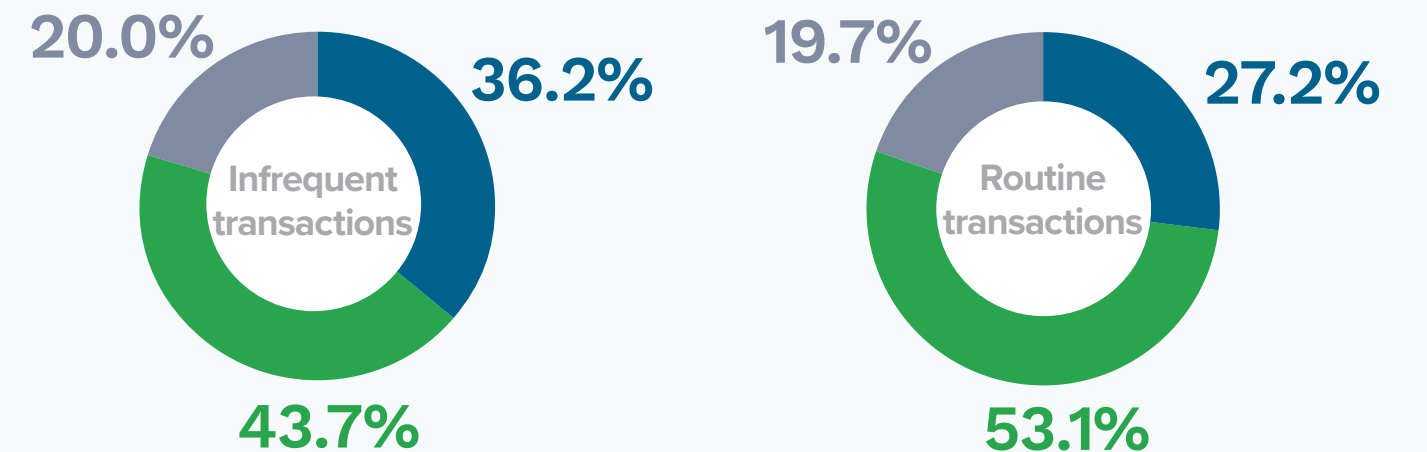
Consumers are most concerned about security when accessing their bank accounts. Among routine online financial activities and transactions, 30% of consumers said they want more visible security measures when accessing accounts, 29% said the same for sending or receiving money and 27% when paying for goods and services. Bill-paying consumers share this sentiment, with 26% preferring more visible security measures when paying bills, rent and loans.

We found some surprising generational differences among consumers who strongly prefer visible security measures for routine activities and transactions.¹ Millennials are most interested in

FIGURE 1:
Consumers' preferences for additional security measures

Share of consumers agreeing with select statements about security measures, by transaction category

- I would like more visible security measures.
- I am comfortable with the current security measures.
- I would like more invisible security measures.



Source: PYMNTS
Consumer Authentication Preferences for Online Banking and Transactions, January 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

visible security measures, with 37% saying they want their FI to implement additional measures. Similar shares of Gen Z and Gen X consumers want additional visible security measures, at 30% and 28%, respectively. Just 16% of baby boomers and seniors said the same.

¹ Within this report, generations are defined as follows: Members of Generation Z are 18 to 26 years old; millennials are 27 to 42 years old; bridge millennials are 35 to 45 years old; members of Generation X are 43 to 58 years old; and baby boomers and seniors are 59 years or older.

Seeing is believing: Visible security and trust

Visible security measures require active user engagement, typically via password-based, multifactor and biometric authentication. This interaction has an outsized impact on consumer perceptions of the safety of their financial information and assets when conducting online financial activities. Our latest research found that just 44% of consumers who bank and transact online think their FIs have adequate security measures for high-risk or infrequent transactions, and 36% want their banks to implement additional visible security measures in these cases.

The preference for more visible security measures varies slightly across different online financial activities and transactions. We discovered that 38% of consumers want more visible security when accessing their bank accounts from a new device, followed closely by 37% who said the same for online transactions involving large sums. Thirty-five percent also want additional visible safeguards when making changes to their personal bank account information online or completing their first online transaction with a given merchant.

The desire for more visible security measures is broadly consistent across demographic groups. When completing infrequent financial activities, 44% of millennials, 40% of Gen Z and 38% of Gen X want additional visible security measures.

FIs must take consumers' preferences for increased visible security measures seriously. Notably, 63% of consumers who prefer more visible security measures said they would feel more confident in the safety of their money if their FI increased visible security measures. FIs could see customers lured away by competitors that offer more visible security.

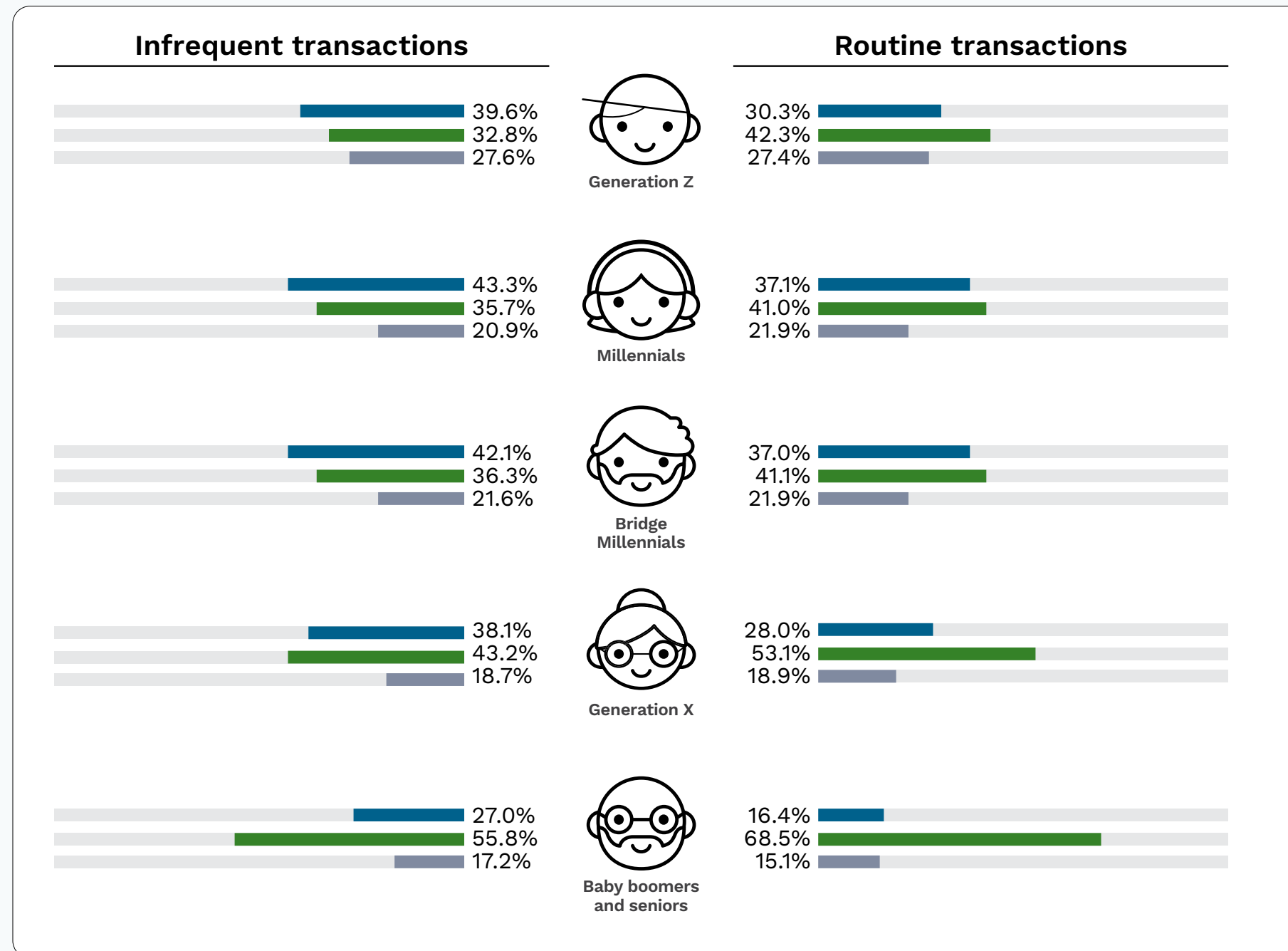
36%

Share of consumers who want their banks to implement additional visible security measures for higher-risk transactions

FIGURE 2:
Preferred security measures

Share of consumers agreeing with select statements about their FIs' security measures, by generation and transaction category

- I would like more visible security measures.
- I am comfortable with the current security measures.
- I would like more invisible security measures.



42%

Share of consumers who feel comfortable with their FIs' current security measures for routine transactions

Source: PYMNTS
Visible and Invisible Security: Perceptions in Digital Banking, March 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

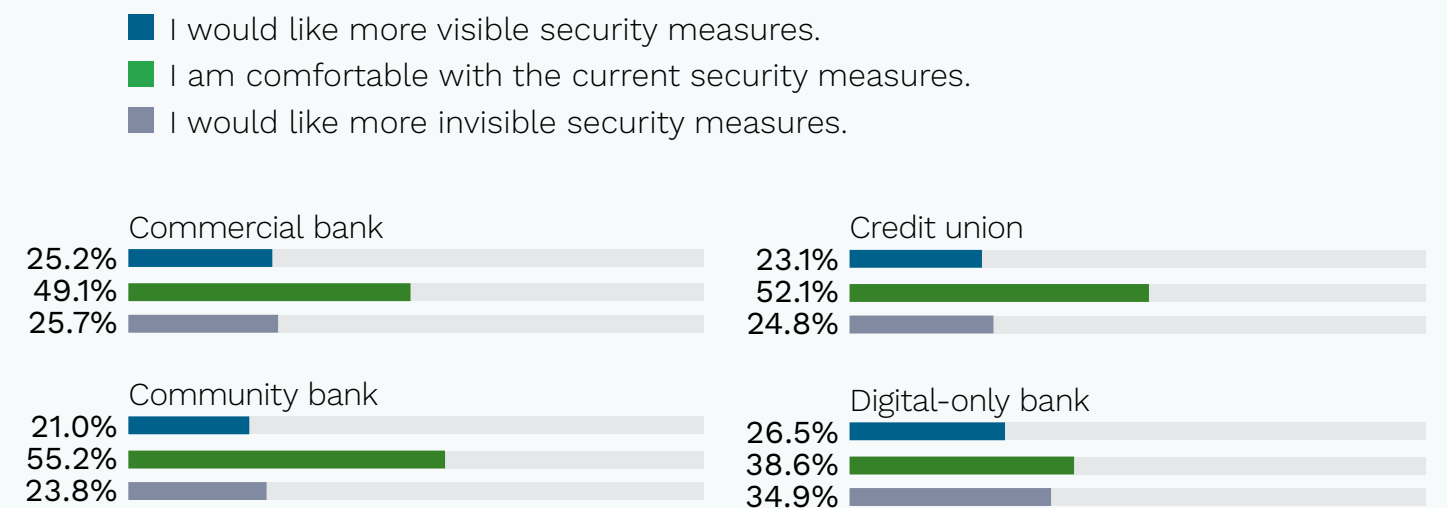
The security mandate: More measures, visible and invisible

The rise of digital-only banks has reshaped the consumer banking landscape, and understanding the preferences of consumers who choose these FIs is crucial. Our data reveals that just 39% of digital-only bank customers feel satisfied with the security status quo. The remainder splits into two camps: 35% would prefer additional invisible security measures, while 27% would prefer additional visible security measures.

Commercial bank customers also show low overall satisfaction with the level of security their FIs provide. Just 49% feel comfortable with the current security measures available, while 25% prefer to expand visible security measures and 26% prefer more invisible security. Community banks and credit unions exhibit broadly the same trend, though with slightly higher levels of customer satisfaction.

FIGURE 3:
Security preferences across banks

Share of consumers agreeing with select statements about their FIs' security measures, by type of primary FI



Source: PYMNTS
Visible and Invisible Security: Perceptions in Digital Banking, March 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

For digital-only banks and traditional FIs, visible security measures take center stage with consumers when asked specifically about non-routine transactions and activities. For example, our data shows that 41% of all commercial and digital-only bank customers want additional visible security measures required the first time a device accesses their bank account. Notably, digital-only bank customers show somewhat more interest than traditional bank customers in having more visible security measures when using the same device to reaccess the same account, at 34% for digital-only customers and 31% for commercial bank customers. This data underscores the critical role of visible security measures for digital-only banks in expanding their retail customer base.

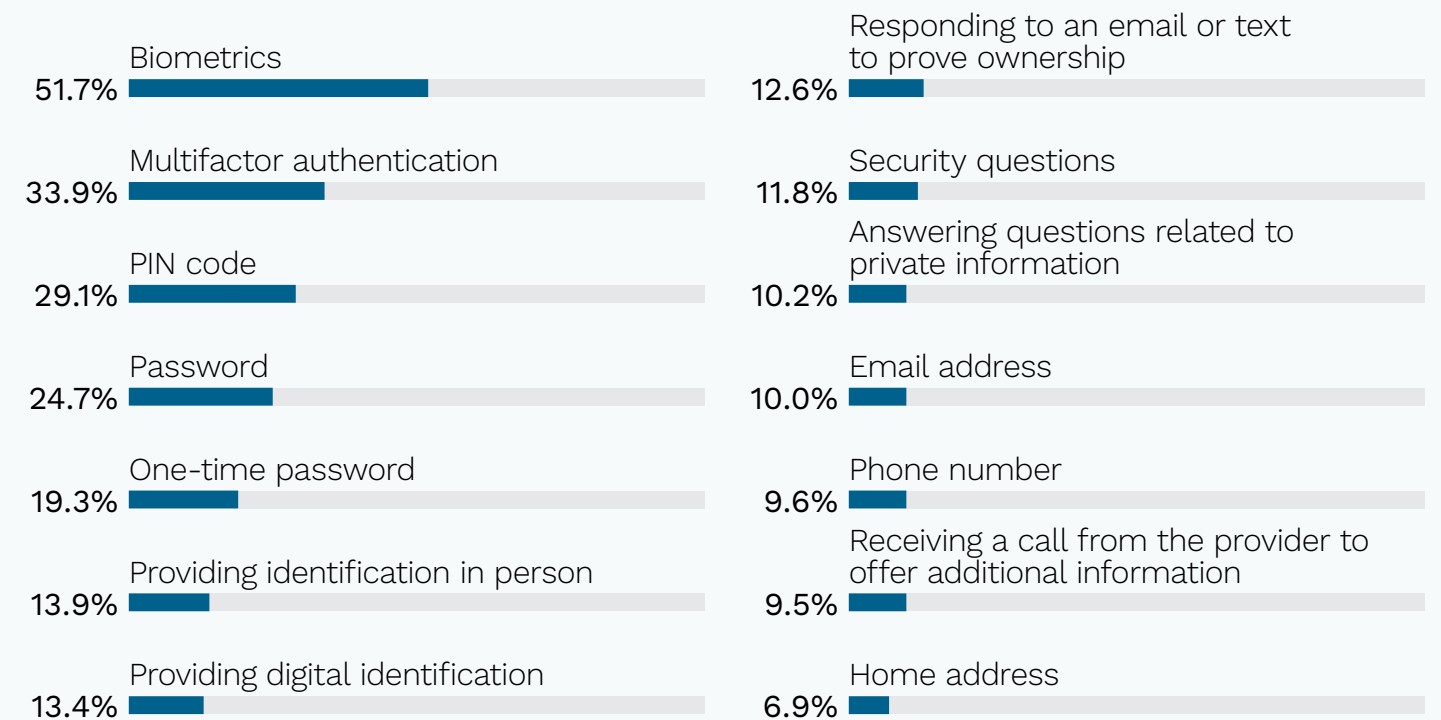
The power of passwordless methods

The old-fashioned password persists as the most common way to authenticate digital financial transactions and activities — but consumers see the myriad shortcomings. While 65% of consumers verified at least one online financial activity or transaction with a password in the last month, 25% of those who have used passwords prefer this authentication method.

Biometrics are rapidly catching up, and most consumers who use this method feel satisfied with it. Our data shows that 47% of consumers authenticated at least one online financial activity or transaction using biometrics in the last month and that 52% of this group would prefer this method over any other form of authentication. Moreover, 31% of all respondents believe that biometric authentication provides the most secure form of online identity authentication — ahead of all other methods.

FIGURE 4:
Consumers' use of and preference for authentication methods

Share of consumers who have used select authentication methods and cite this method as their most preferred method



Source: PYMNTS
Consumer Authentication Preferences for Online Banking and Transactions, January 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

47%

Share of consumers who used biometric authentication for online financial activity in the last month

FIs must find the right mix of security, ease of use and convenience to satisfy consumers. Our data reveals that 68% of consumers who prefer biometric authentication cite convenience as the primary reason for their preference, and 67% cite ease of use, significantly higher than the 44% who cite security.

MFA is the second-most preferred method for online authentication, with 34% of consumers who used this method in the past month preferring it over others. However, consumers find MFA less easy to use and convenient than using exclusively biometric authentication, with just 42% of consumers saying they choose MFA because it is easy and 33% of users reporting they choose it because it is convenient. Sixty-two percent of consumers who choose MFA believe it provides stronger security.



52%

**Share of consumers
who prefer biometric
authentication, among
those who used
this method in the
last month**

Conclusion

Many consumers feel dissatisfied with the security status quo for online financial transactions and banking activities. Customers of traditional and digital-only banks alike want their FIs to do more to protect their assets and personal information — and visible security measures play a unique role in their perceptions and experience. FIs can significantly boost customer satisfaction and engagement by offering a suite of visible security measures and allowing customers to choose additional security steps for certain activities, such as high-value transactions and logins from new devices. Consumers particularly want biometric authentication, which could soon replace passwords as the go-to verification method, and MFA options, which they widely view as providing extra layers of security. In short, consumers want to own their experience, and personalization options are crucial to making that happen. In doing so, FIs should consider partnering with a third-party specialist that can deliver the solutions they need to optimize their approach to visible security.

Methodology

Visible and Invisible Security: Perceptions in Digital Banking, a PYMNTS and Entersekt collaboration, is based on a population-balanced study of 2,584 U.S. consumers fielded between Sept. 26, 2022, and Oct. 3, 2022, that examined consumers' preferences for visible and invisible online authentication methods. The sample was balanced to match the U.S. adult population in key demographic variables.

About

Disclaimer

PYMNTS [PYMNTS](#) 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.

Visible and Invisible Security: Perceptions in Digital Banking may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS 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 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 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 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 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 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 is the property of PYMNTS 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.