PYMNTS | entersekt

Retail Banking Security:

Consumer Behavior in Focus

May 2023

Retail Banking Security: Consumer Behavior in Focus, 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.

Retail Banking Security:

Consumer Behavior in Focus

Table of Contents

Retail Banking Security: Consumer Behavior in Focus was produced in collaboration with Entersekt, and PYMNTS is grateful for the company's support and insight. PYMNTS retains full editorial control over the following findings, methodology and data analysis.

PYMNTS | entersekt

Introduction

Although many of the recent innovations in banking and transacting have emphasized convenience, PYMNTS' data finds that retail banking customers have become concerned about the safety of their personal and financial information when banking and transacting online to the extent that most would willingly trade convenience for more security measures. Millennials and higher-income consumers disproportionately favor stronger safeguards, even when those measures add steps to a transaction.

Consumers want control and safety, and this extends vicariously to their banking institutions. Our research finds that consumers are willing to share their personal information with financial institutions (FIs) and then allow those FIs to share that information with providers to enhance the security of their online transactions. Millennials and Gen Z stand out in this regard, with 53% and 49%, respectively, open to allowing their FIs to share personal and financial data with existing service providers to boost security.

Notably, customers of digital-only banks are more inclined to share this data than those who bank with traditional FIs, highlighting how trust is evolving among two very different types of account holders — and that digital banks may have an upper hand in a world besieged by digital threats.

As worries about these security threats continue to multiply, banks must prioritize robust security measures and give their customers the control and transparency they want. Retail Banking Security: Consumer Behavior in Focus, a PYMNTS and Entersekt collaboration, examines consumers' data security concerns when transacting online, preferences for convenience versus security, and willingness to share personal information with FIs to bolster online transaction security. 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 are highly concerned about the security of their data when using online financial service accounts.

Sixty-nine percent of retail banking consumers fear their personal and financial data is vulnerable to digital security threats, with 39% deeply concerned. Millennials and bridge millennials are the most likely to be highly worried about the vulnerability of their assets and information, and a substantially larger share of high-income consumers are more deeply concerned than middle- and lower-income groups.

Millennials prioritize security over convenience in online banking.

Sixty-two percent of all banking customers prioritize security over convenience, with 60% citing protection of their identity and money as the top reason for holding this view. Millennials and bridge millennials lead this trend, at 66% and 67%, respectively, while 52% of Gen Z consumers also lean toward greater security. We also find that consumers in higher income brackets tend to be more willing to sacrifice convenience for better security.

A much higher share of consumers is willing to permit their FIs to share personal data with familiar service providers to enhance security than with unfamiliar ones.

To enhance online transaction security, 41% of consumers are open to allowing their FIs to share sensitive personal data with their existing insurance providers, 43% with their existing health insurance providers, and 38% with technology companies with which they already have an account. However, when it comes to permitting the release of sensitive information to unfamiliar providers, the share of willing consumers drops to just one in four.

Customers of digital-only banks are much more likely than those of traditional FIs to be willing to allow those entities to share personal information with service providers.

The same forward-looking consumers who embrace digital-only banks also tend to be far more willing than their peers to allow their FIs to share private information with service providers to improve security. For example, 50% of digital-only bank customers said they would permit the sharing of data with their current insurance providers, versus only 36% to 44% of consumers who bank with traditional FIs. This pattern holds for new providers as well, though the numbers are lower across the board.

PYMNTS | entersekt

Security in consumers' minds

PYMNTS' latest consumer research reveals that nearly 7 in 10 retail banking customers worry their sensitive personal and financial data may be vulnerable to digital security threats when they use financial services online. Thirty-nine percent are deeply concerned. FIs must effectively address this widespread unease to best attract new customers and retain existing ones.

Millennials and bridge millennials — often valuable demographics, given that many are in their peak earning years — are especially alarmed about potential data vulnerability. Respectively, 47% and 51% are deeply concerned about online security. While those demographics lead the field, the drop off to other generations is not large: 40% of Generation X and 37% of baby boomers and seniors share this alarm. A smaller but still sizable share of digitally native Generation Z consumers — 29% — also report being highly worried.

TABLE 1:

Consumers' security concerns
Share of consumers expressing select levels of concern about the security of their private data, by demographic

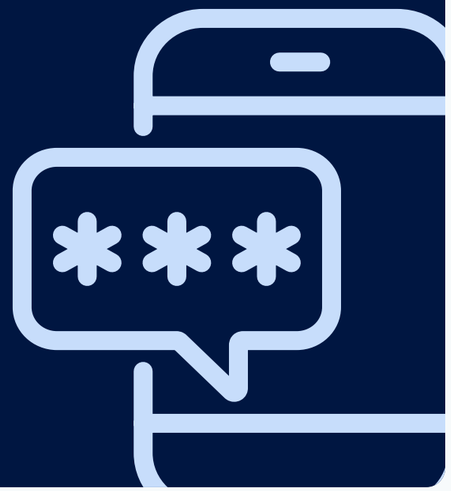
	LEVEL OF CONCERN		TOTAL
	Very or extremely concerned	Somewhat concerned	
SAMPLE	**39.4%**	**29.4%**	**68.9%**
FINANCIAL LIFESTYLE			
• Do not live paycheck to paycheck	35.6%	30.1%	**65.7%**
• Live paycheck to paycheck without issues paying bills	37.9%	32.3%	**70.2%**
• Live paycheck to paycheck with issues paying bills	44.6%	24.8%	**69.4%**
INCOME			
• More than $100K	46.9%	26.7%	**73.6%**
• $50K-$100K	35.9%	30.2%	**66.1%**
• Less than $50K	34.1%	31.9%	**66.1%**
GENERATION			
• Generation Z	28.6%	31.4%	**60.0%**
• Millennials	46.7%	24.3%	**71.1%**
• Bridge millennials	50.6%	20.5%	**71.1%**
• Generation X	39.6%	28.3%	**67.9%**
• Baby boomers and seniors	36.8%	34.3%	**71.0%**

Source: PYMNTS
Retail Banking Security: Consumer Behavior in Focus, May 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

If the widespread multigenerational concern is not enough to kick FIs into high gear, an analysis of income brackets and this unease might. High-income consumers — those earning more than $100,000 per year — are particularly likely to worry about the security of their personal data and financial assets; 47% are highly concerned. The corresponding shares of middle-income (earning $50,000 to $100,000) and lower-income (earning less than $50,000) consumers are much closer to one-third (36% and 34%, respectively).

47%

of high-income consumers are highly concerned about the security of their personal data and financial assets.



69%

of retail banking customers worry their sensitive personal and financial data may be vulnerable when they use financial services online.

All in all, this data underscores the pressing need for banks to assure their customers and prospective account holders of the security of their personal and financial data.

PYMNTS | entersekt

For most, security trumps convenience

Convenience no longer drives retail banking customers' preferences — not when their sensitive personal and financial information is on the line. PYMNTS' research shows that the scales have tipped, with 62% of all retail banking consumers willing to sacrifice convenience for hardened security safeguarding their sensitive personal information and assets.

Across every age group except for Gen Z, more than 60% of retail banking consumers opt for heightened security over convenience. Millennials and bridge millennials lead the way, with 66% and 67%, respectively, prioritizing security over convenience. While a sizable share of Gen Z consumers holds a different perspective — 39% express satisfaction with their banks' current balance of convenience and security — 53% still lean toward greater security over convenience.

TABLE 2:

The balance of convenience and security
Share of consumers expressing select sentiments about convenience and security trade-offs, by demographic

	Give up convenience to gain security	Satisfied with the balance	Give up security to gain convenience
SAMPLE	**61.7%**	**33.2%**	**5.1%**
FINANCIAL LIFESTYLE			
• Do not live paycheck to paycheck	65.4%	30.6%	4.0%
• Live paycheck to paycheck without issues paying bills	61.2%	33.4%	5.5%
• Live paycheck to paycheck with issues paying bills	59.6%	34.9%	5.5%
INCOME			
• More than $100K	67.4%	28.3%	4.3%
• $50K-$100K	61.2%	34.7%	4.1%
• Less than $50K	55.7%	37.3%	7.0%
GENERATION			
• Generation Z	52.7%	39.1%	8.3%
• Millennials	65.7%	30.3%	4.0%
• Bridge millennials	66.8%	29.6%	3.6%
• Generation X	60.5%	34.0%	5.5%
• Baby boomers and seniors	62.5%	32.8%	4.7%

Source: PYMNTS
Retail Banking Security: Consumer Behavior in Focus, May 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

Similar to the patterns in our data about security concerns, consumers with higher incomes tend to be the most willing to prioritize security over convenience. While 56% of low-income banking customers are ready to ditch convenience for better security, this share climbs to 67% among high-income earners. As digital security threats proliferate and consumers take notice, banks must demonstrate that they are being vigilant.

62%

of all retail banking customers are willing to sacrifice convenience for better security.

PYMNTS | entersekt

Consumers trust the familiar

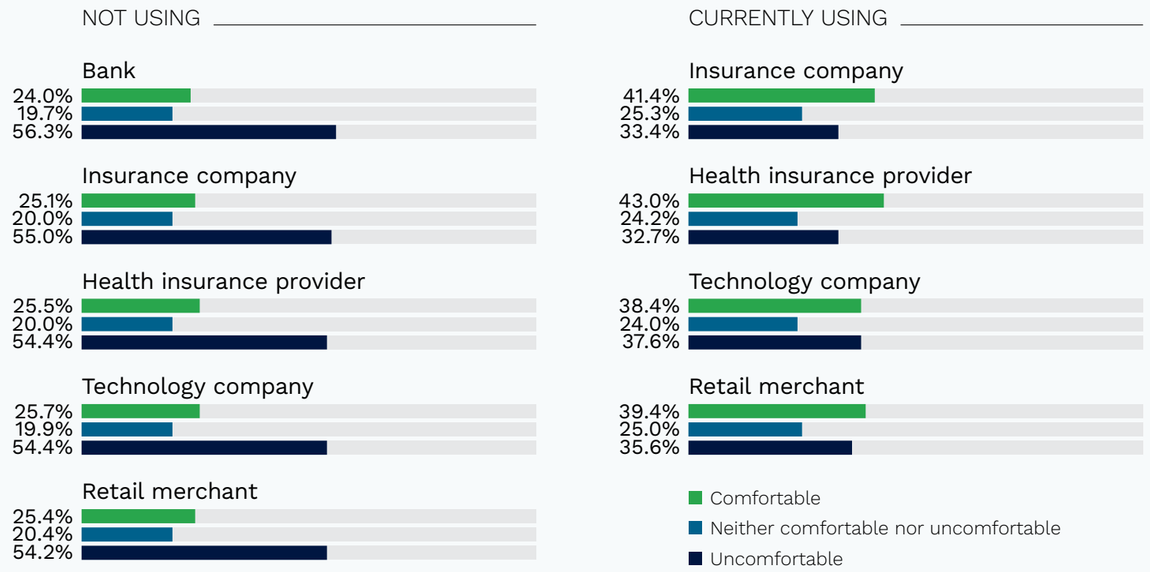
PYMNTS' data shows that privacy-conscious consumers are willing to allow their FIs to share sensitive personal information with existing service providers they trust, provided that doing so ultimately bolsters the security of their online transactions.

Diving deeper into the data, 41% of consumers are open to permitting the disclosure of their sensitive information to their current insurance providers to enhance security. We discovered that even technology companies — often criticized for privacy concerns — can gain this level of trust with 38% of their users if they deliver more secure online transactions. However, for providers with whom consumers have no relationship, just 1 in 4 consumers are comfortable allowing their information to be released.

FIGURE 1:

Consumers' willingness to allow FIs to share their personal data for security

Share of consumers with select comfort levels in permitting their FIs to share personal data with specific providers if it makes transactions more secure



Source: PYMNTS
Retail Banking Security: Consumer Behavior in Focus, May 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

Millennials are the most willing to have their sensitive data shared with current providers to boost transaction security, at 53%, followed by Gen Z, at 49%. Forty percent of Gen X share this outlook, while baby boomers and seniors are more skeptical, at 26%. We note that, despite an overall cautious stance toward sharing sensitive information with unfamiliar service providers, 37% of millennials are still prepared to forego privacy with providers they do not currently use for enhanced security.

PYMNTS | entersekt

Customers of digital-only banks lead the pack

Technology-savvy consumers who embrace digital banks tend to be more open-minded about sharing private information than those who primarily bank with traditional FIs.

For example, 50% of digital bank customers are willing to hand over personal data via their FIs to their current insurance providers in exchange for enhanced transaction security — a much higher share than account holders at credit unions (37%), community banks (36%) or large traditional banks (44%). We found similar trends for health insurance providers specifically, as well as technology providers and retail merchants, with digital-only bank customers much more likely than the rest to be willing to share personal information.

50%

of digital bank customers are willing to permit their FIs to share personal data with their current insurance providers for enhanced transaction security.

TABLE 3:

Account holders' willingness to share data with familiar providers

Share of consumers who are comfortable having their personal data shared with providers they already use, by type of primary bank

	Credit union	Community bank	Commercial bank	Digital-only bank
• **Retail merchants with existing account/profile**	33.2%	36.4%	40.6%	52.5%
• **Technology company with existing account/profile**	32.9%	34.3%	39.7%	51.3%
• **Current health insurance provider**	37.4%	39.9%	45.2%	**53.3%**
• **Insurance company**	37.4%	36.4%	44.0%	50.2%

Source: PYMNTS
Retail Banking Security: Consumer Behavior in Focus, May 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

Across the board, consumers are less likely to trust new service providers with sensitive information, but those who use digital-only banks are much more open to doing so than their peers. For new insurance providers, 33% of the digital-only bank group indicated being willing to share personal information to improve security, versus just 23% to 25% of those who bank with traditional FIs.

TABLE 4:

Account holders' willingness to share data with new providers

Share of consumers who are comfortable having their personal data shared with providers they do not already use, by type of primary bank

	Credit union	Community bank	Commercial bank	Digital-only bank
• Retail merchants without existing account/profile	23.9%	21.2%	25.5%	35.4%
• Technology company without existing account/profile	24.2%	22.3%	25.2%	**37.6%**
• Current health insurance provider	24.5%	22.7%	25.3%	34.8%
• Insurance company	23.9%	22.5%	25.3%	32.9%
• Bank	21.6%	22.3%	24.2%	32.1%

Source: PYMNTS
Retail Banking Security: Consumer Behavior in Focus, May 2023
N = 2,584: Complete responses, fielded Sept. 26, 2022 – Oct. 3, 2022

Across the board, consumers who use digital-only banks are much more open to trusting new service providers with sensitive information than peers who bank elsewhere.

Conclusion

The ever-more-complex landscape of digital financial services has left consumers increasingly concerned about the security of their personal and financial data. The growing unease extends across age groups and income levels, pushing the majority of banking customers to consider trading some convenience for stronger safeguards. This mindset extends to sharing personal data with trusted providers, and digital bank customers are especially receptive to this exchange, though they, too, have their limits. FIs must take these concerns seriously and prioritize the implementation of robust security measures while also empowering customers with greater control over sharing their personal and financial data.

Methodology

Retail Banking Security: Consumer Behavior in Focus, 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

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.

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.

Disclaimer

Retail Banking Security: Consumer Behavior in Focus 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.