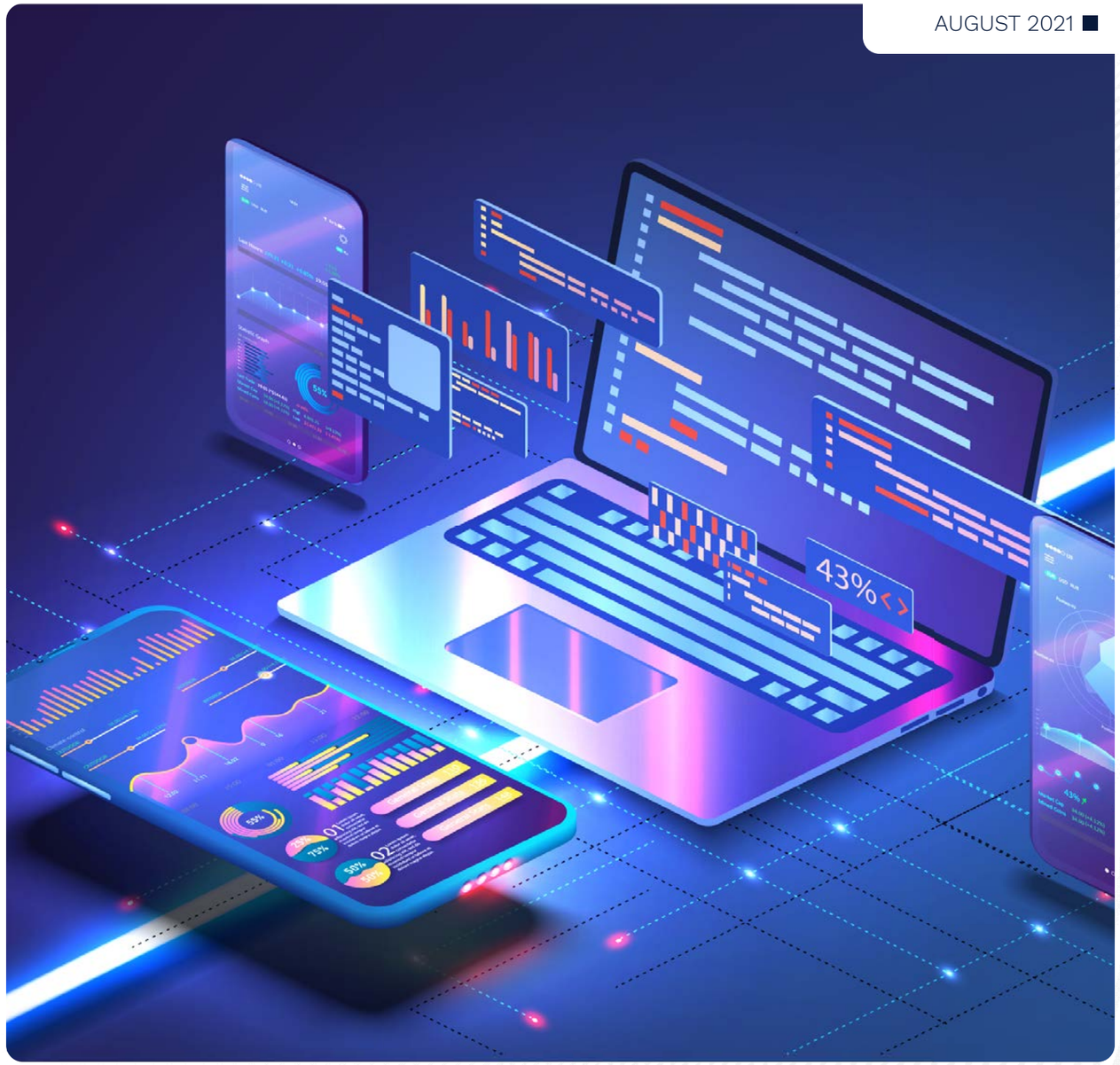
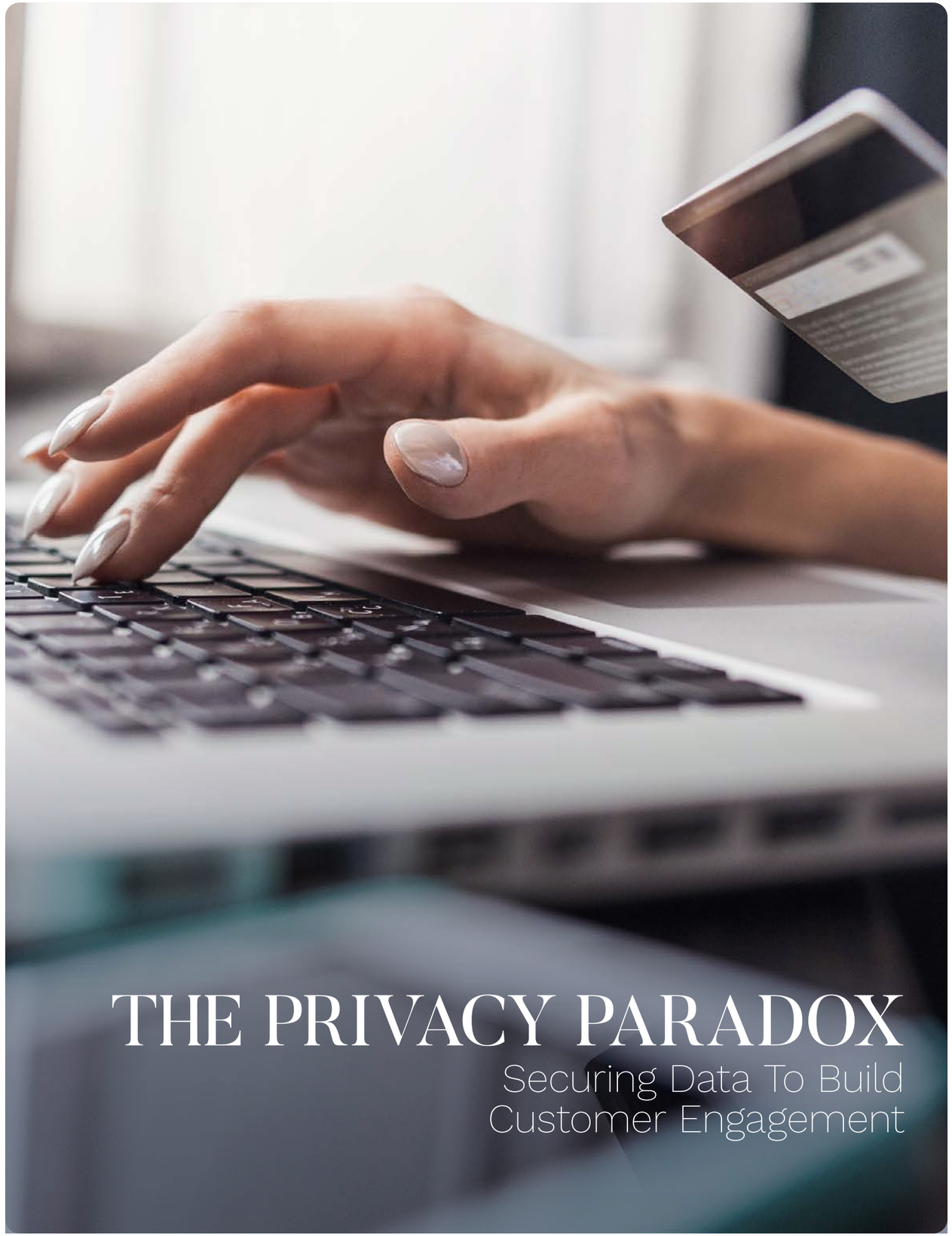
The Privacy Paradox: Securing Data To Build Customer Engagement, a PYMNTS and Very Good Security collaboration, examines the role of personally identifiable information (PII) protections in customer engagement and offers insights into how companies can better address consumers' concerns around data privacy. The report is based on a survey of 2,257 U.S. consumers.



THE PRIVACY PARADOX

Securing Data To Build Customer Engagement

PYMNTS.com | VERY GOOD SECURITY



THE PRIVACY PARADOX

Securing Data To Build Customer Engagement

Table of Contents

PYMNTS.com | VERY GOOD SECURITY

The Privacy Paradox: Securing Data To Build Customer Engagement was done in collaboration with Very Good Security, 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

Consumers began conducting more of their lives digitally in 2020 due to the health crisis, and though aspects of the country are reopening, consumers remain more active online than ever. The overwhelming majority — 85 percent — of those who transferred the bulk of their shopping activities to digital channels plan to keep performing at least one digitally "shifted" task, even when restrictions on retail locations end.[1] Merchants will have to manage online personal data securely for the foreseeable future — and at a historic scale.

The FBI reported a 400 percent increase in cyberattacks on personal data in 2020 as consumers brought their shopping and banking activities online.[2] The challenge of secure data management gained prominence as consumers have learned more about how their data might be mishandled or stolen by bad actors.

Consumers also consider data security when they are asked to surrender sensitive information in person — even by their banks, which consumers tend to view as more trustworthy than retailers, according to research.[3] A recent survey revealed that 64 percent of consumers are always thinking about the security of their data whenever they interact with their financial institutions, and 57 percent have begun thinking about it more since the health crisis began.[4]

Consumers' overwhelming interest in keeping their personal information secure wherever they might encounter a risk of data compromise has real-world ramifications for retailers. Another recent survey revealed that 87 percent of consumers would refuse to do business with a company if they had doubts about the way the company might handle their data.[5] PYMNTS' researchers found that 85 percent of consumers used merchant trustworthiness in managing their data and protecting them from fraud as a key determinant of where they will shop.[6]

The paradox facing merchants is significant: Consumers want highly secure interactions that protect their data, but they also want customized, frictionless checkout experiences, which are often powered by that data. Merchants, having increased their investments in data security by 68 percent in 2020, must find a solution that protects customer data and assures consumers that their details are safe.

In The Privacy Paradox: Securing Data To Build Customer Engagement, a collaboration with Very Good Security, PYMNTS examines the results of a survey of 2,257 United States consumers to reveal the role of personally identifiable information (PII) protections in customer engagement. This report provides insights into steps that companies can take to address consumers' concerns about data privacy.

[1] Inside The Mind Of The Digital-First Consumer. PYMNTS.com. 2021. https://www.pymnts.com/digital-payments/2021/inside-the-mind-of-the-digital-first-consumer/. Accessed July 2021.

[2] Miller, M. FBI sees spike in cyber crime reports during coronavirus pandemic. The Hill. 2020. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic. Accessed July 2021.

[3] Bruce, G. Global data: Which sectors do consumers trust most with their personal data? YouGov. 2021. https://today.yougov.com/topics/technology/articles-reports/2021/04/23/global-data-which-sectors-do-consumers-trust-most-. Accessed July 2021.

[4] Cercelle, T; Sohail, O. Redesigning customer privacy programs to enable value exchange. Deloitte Insights. 2020. https://www2.deloitte.com/content/dam/insights/us/articles/5214_CFS-Privacy/5214_CFS_Privacy_v5.pdf. Accessed July 2021.

[5] Anant, V; Donchak, L; Kaplan, J; Soller, H. The consumer-data opportunity and the privacy imperative. McKinsey & Company. 2020. https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative. Accessed July 2021.

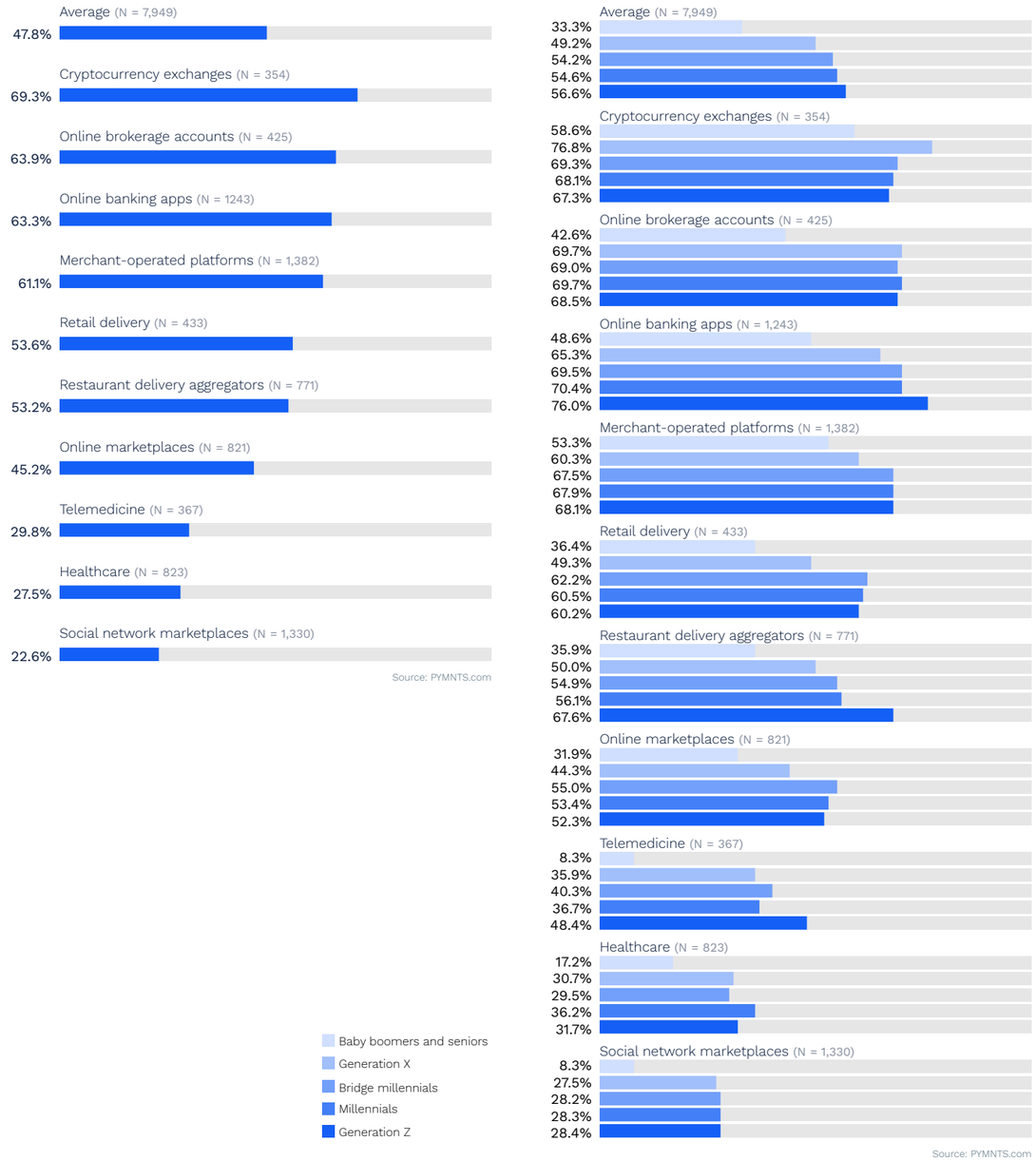
[6] NEW REPORT: How Voice Assistants Help Win Consumer Spend — And Their Trust. PYMNTS.com. 2020. https://www.pymnts.com/news/merchant-innovation/2020/consumer-trust-loyalty-voice-assistant-ecommerce-amazon-pay/. Accessed July 2021.

Popular but not universal: Less than half of consumers currently store payment credentials in their online accounts.

PYMNTS' research found that consumer respondents from younger generations — including Generation Z, millennials and bridge millennials — are the most likely to store payment credentials. Only 48 percent of all survey respondents reported storing their payment credentials in online accounts. Rates were higher for cryptocurrency exchange users (69 percent) and online brokerage users (64 percent), but only 23 percent of social network marketplace users said they store payment credentials. Bridge millennial, millennial and Gen Z consumers were the most likely generations of all to store payment credentials online. PYMNTS discovered that 55 percent of consumers who do not store payment credentials online cite concerns about their payment data being stolen as their reason for not doing so. The largest portions of consumers who choose not to store credentials online and cite this specific concern for why are those using merchant-operated platforms (65 percent), social network marketplaces (61 percent) and online banking apps (59 percent).

THE PRIVACY PARADOX
Securing Data To Build Customer Engagement

FIGURE 1: Consumers' storage of payment credentials on select platforms



Source: PYMNTS.com

TABLE 1:

Why consumers do not store payment credentials on select platforms
Share of consumers who do not store payment credentials expressing select reasons for not doing so, by type of platform

	Worries about payment data being stolen	Worries about losing money	The platform does not allow me to store payment credentials.	Payment credentials must be reentered when transactions occur, anyway.	Do not use often enough or there is no need to	The platform makes it too difficult to store payment credentials.	It is not convenient.	Other
• Average (N = 4,174)	54.6%	11.0%	10.7%	9.2%	7.0%	3.8%	1.3%	2.5%
• Merchant-operated platforms (N = 548)	**64.6%**	11.1%	5.0%	8.9%	2.5%	3.4%	1.2%	3.3%
• Social network marketplaces (N = 1,033)	61.0%	10.3%	8.5%	5.3%	8.8%	3.3%	1.4%	1.2%
• Online banking apps (N = 460)	58.8%	10.4%	8.3%	10.3%	3.5%	3.5%	1.0%	4.2%
• Online marketplaces (N = 450)	58.8%	12.1%	3.5%	**12.8%**	6.3%	3.6%	**1.9%**	1.1%
• Restaurant delivery aggregators (N = 360)	54.9%	14.9%	5.8%	11.4%	4.7%	5.1%	1.1%	2.2%
• Online brokerage accounts (N = 154)	48.8%	14.5%	7.7%	11.7%	4.0%	**8.1%**	1.1%	4.2%
• Retail delivery (N = 201)	48.4%	**16.5%**	5.5%	11.0%	10.2%	3.5%	1.7%	3.3%
• Healthcare (N = 596)	41.0%	7.3%	24.7%	9.8%	**11.2%**	2.5%	0.9%	2.5%
• Cryptocurrency exchanges (N = 113)	39.2%	15.6%	15.4%	10.2%	5.7%	8.0%	0.5%	**5.4%**
• Telemedicine (N = 259)	38.2%	7.1%	**26.0%**	8.8%	10.0%	5.5%	1.3%	3.3%

Source: PYMNTS

Meet the super engagers: affluent, millennial, data security–savvy and deeply connected to their favorite platforms.

Consumers engage 12 times per month with online platforms on average, and millennials and bridge millennials are the most engaged demographic groups. They engage 14 and 13 times per month on average, respectively, whereas baby boomers and seniors only average 10 times per month.

Customer engagement on social network marketplaces almost doubles those rates, with users generally engaging 23 times per month. Engagement on cryptocurrency exchange platforms is 1.5 times the average, at 19 times per month.

FIGURE 2: Average number of times per month users engage with select online platforms

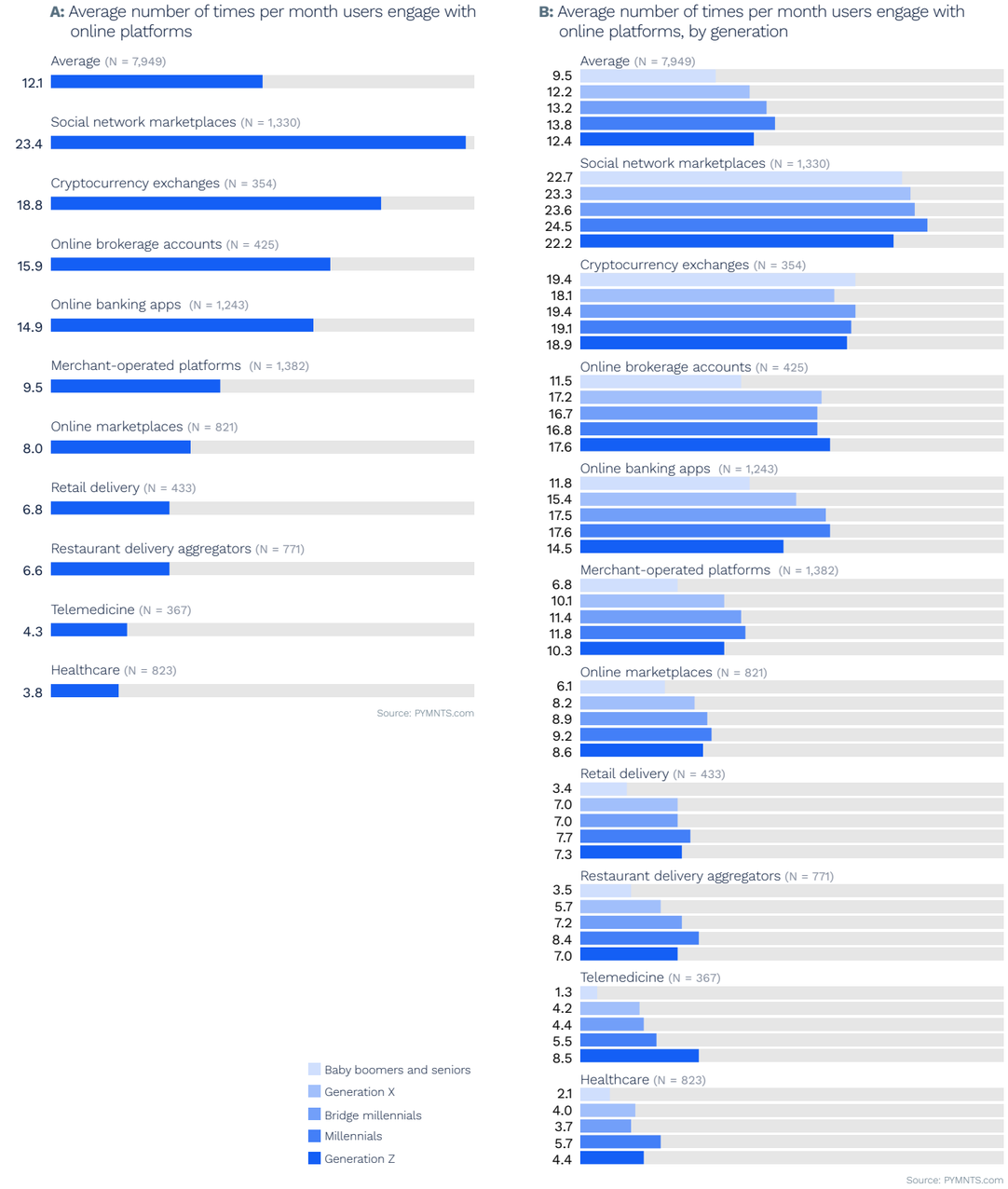
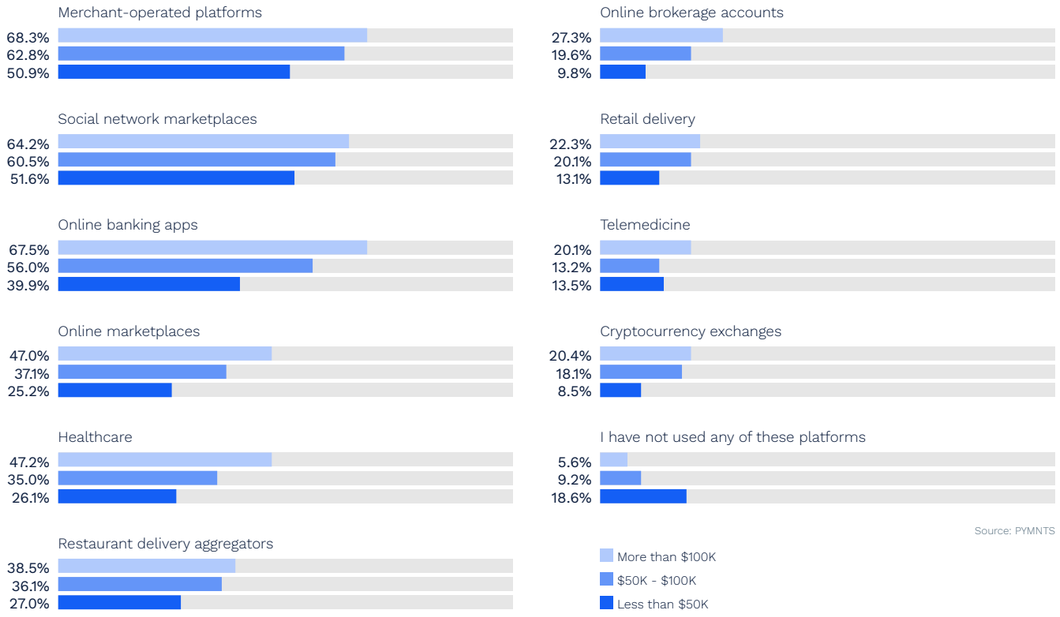


FIGURE 3:

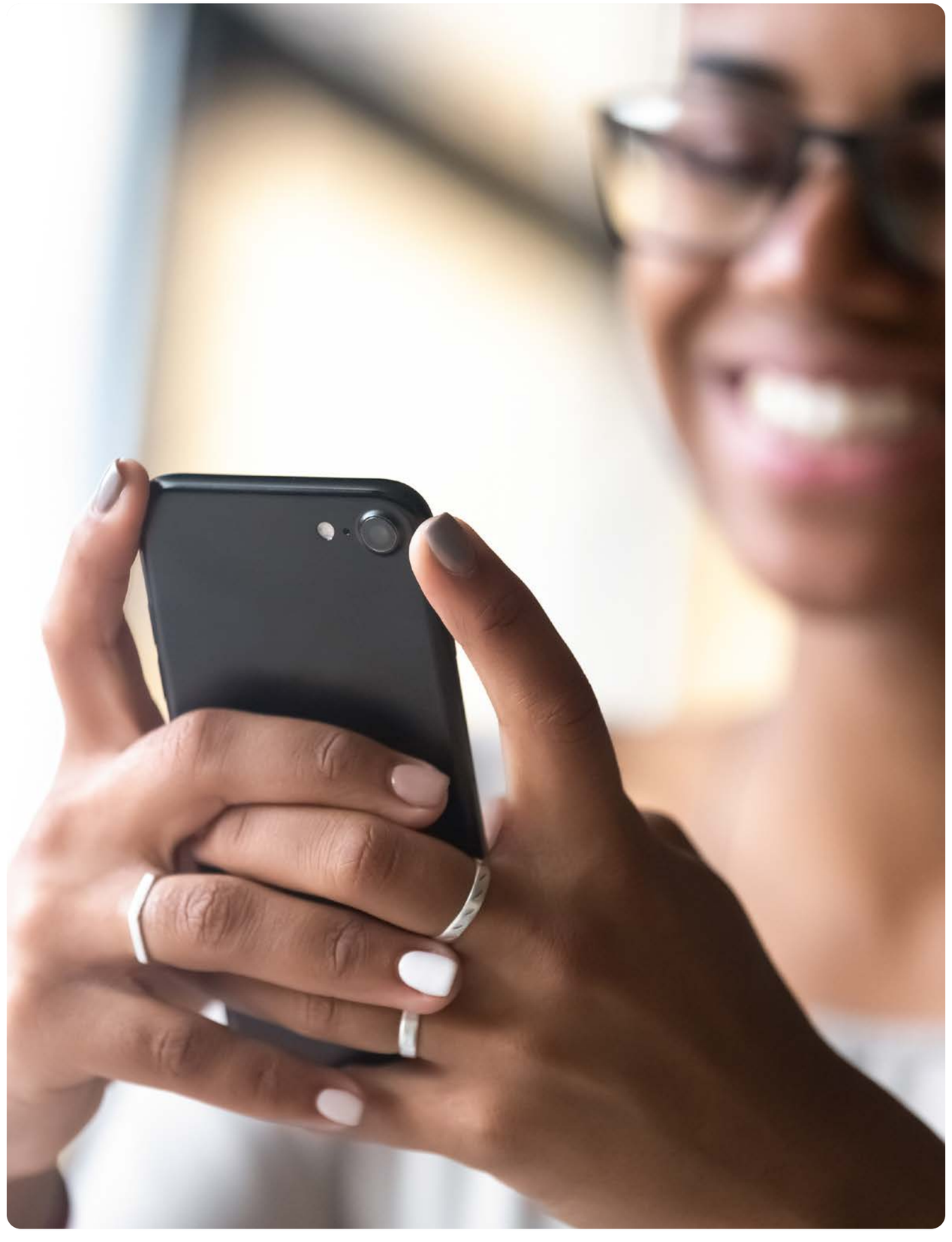
Engagement with online platforms

Share of consumers who have engaged with select online platforms over the last 12 months, by annual income



Source: PYMNTS

Consumers with higher incomes are more likely to engage with online platforms. Survey respondents earning more than $100,000 per year showed the highest levels of engagement with merchant-operated platforms.



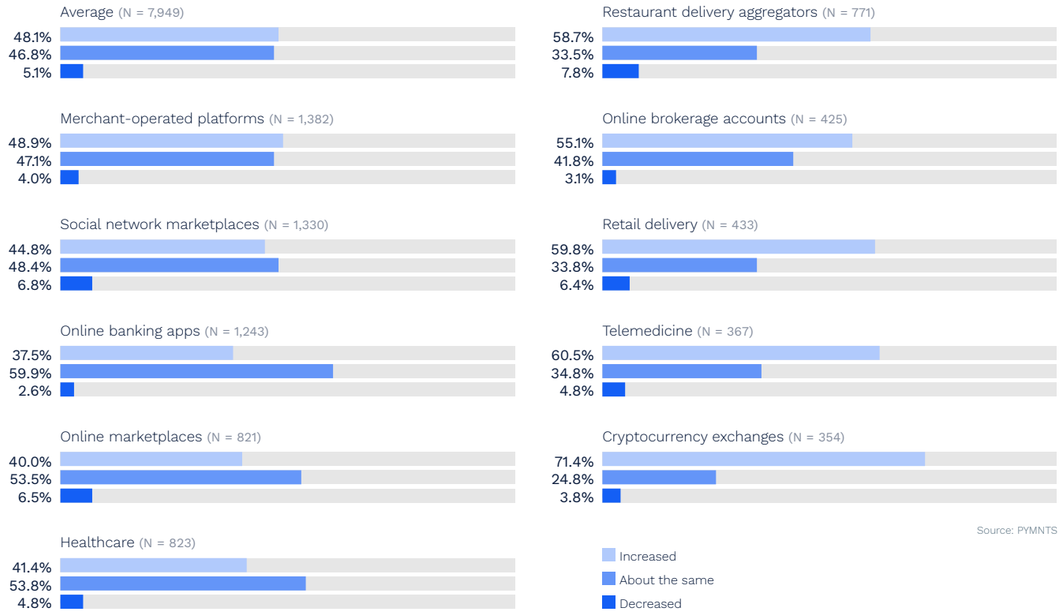
The new fear factor: Consumers used platforms that store PII more, and concerns about data security rose in tandem.

Over the past 12 months, large shares of consumer respondents increased their use of platforms that manage cryptocurrency transactions (71 percent), telemedicine services (60 percent), retail delivery (60 percent), restaurant delivery aggregators (59) and online brokerage accounts (55 percent). Consumers' concerns over sharing their PII often relate to specific fears about data misuse, and there are generational differences as to why consumers are worried about data handling. Our researchers found that nearly all consumers exhibit some concern about the security of their PII online, with 81 percent at least "somewhat" concerned about providing PII to access online accounts and 49 percent "very" or "extremely" concerned.

THE PRIVACY PARADOX
Securing Data To Build Customer Engagement

FIGURE 4:

Change in frequency of consumer engagement with select online platforms
Share of consumers who have increased or decreased their frequency of engagement with select online platforms over the last 12 months



Source: PYMNTS

FIGURE 5: Consumers' concern about providing PII to access online platform accounts

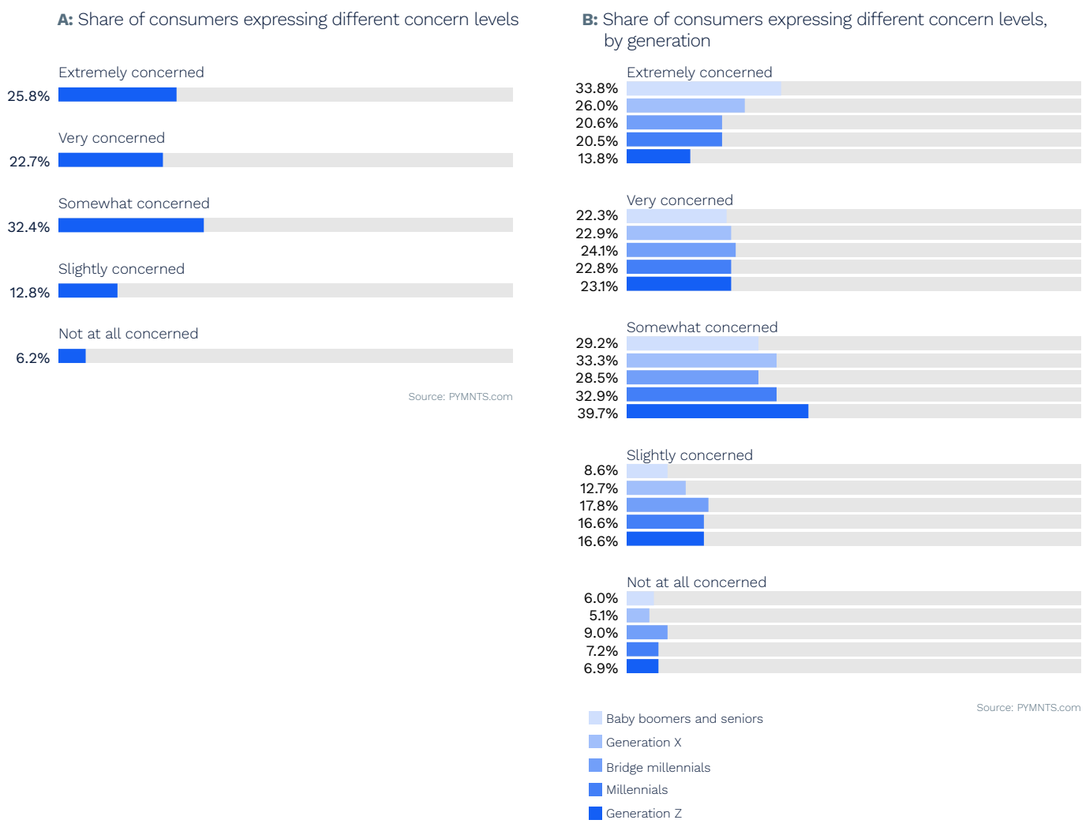
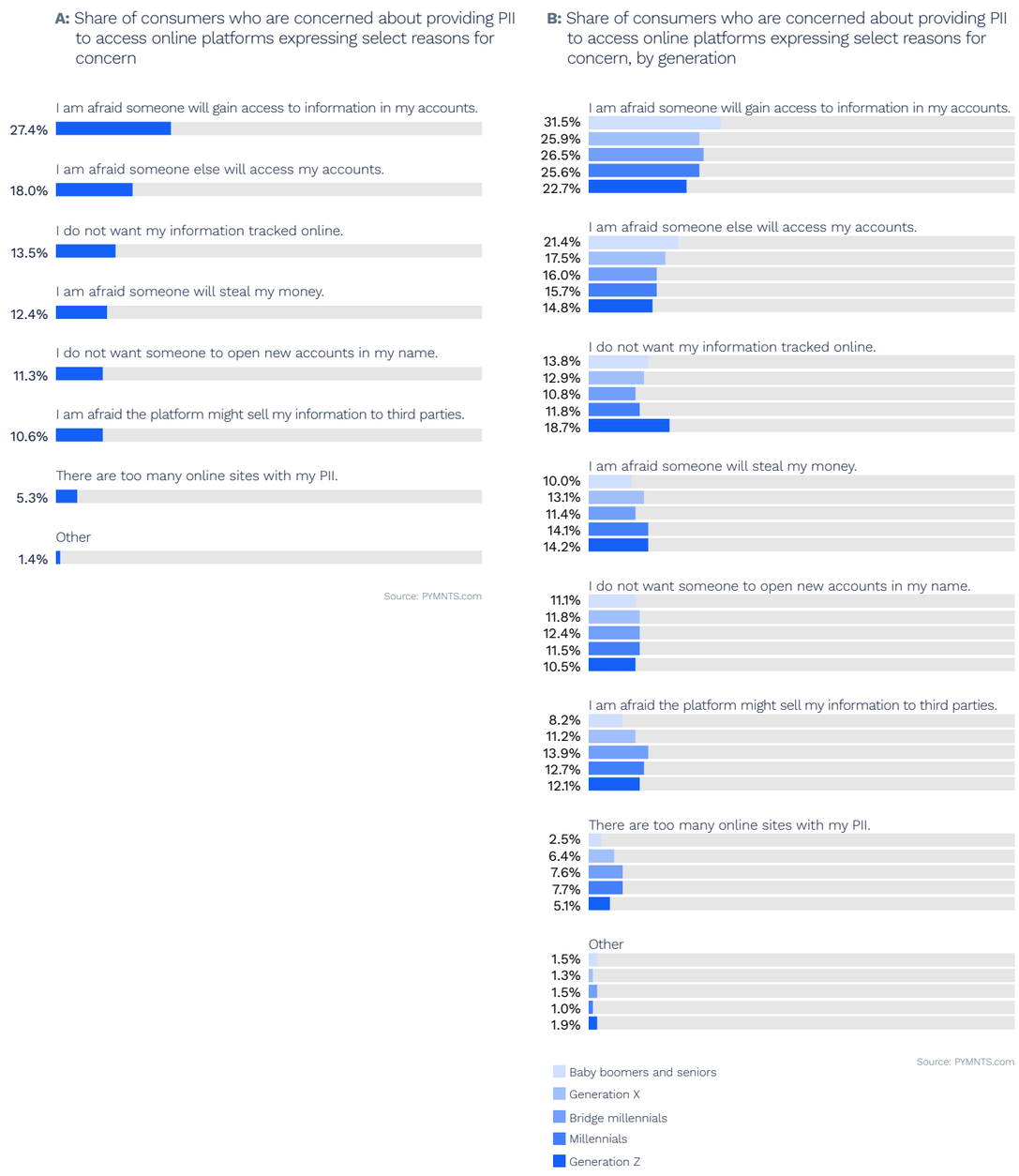


FIGURE 6: Reasons for concern about providing PII



Consumer concerns about PII are often focused on platform breaches that can lead to data theft or unauthorized data access by criminals or other parties. Our data revealed the extent of Americans' fears over data theft: an aggregated 45 percent of consumers said they are afraid to share their PII either because they are worried about someone accessing their accounts (18 percent) or the personal information stored in them (27 percent). We found that 55 percent of consumers who do not store payment credentials with a merchant are worried about their payment data being stolen.

From worry to walkout:
Concerns over PII lead to merchant or platform abandonment.

Our researchers found that data protection is a key factor affecting customer engagement with a merchant or platform. PYMNTS' data shows that 57 percent of consumers would be highly likely to switch to another online platform if they became concerned about a provider sharing or not protecting their PII. This share increased to 62 percent among baby boomers and seniors. Crucially, 65 percent of consumers were very likely to abandon a cart or stop an account sign-up process if they felt concern about the security of their personal information.

FIGURE 7: How concern about a platform not protecting or sharing PII can trigger abandonment

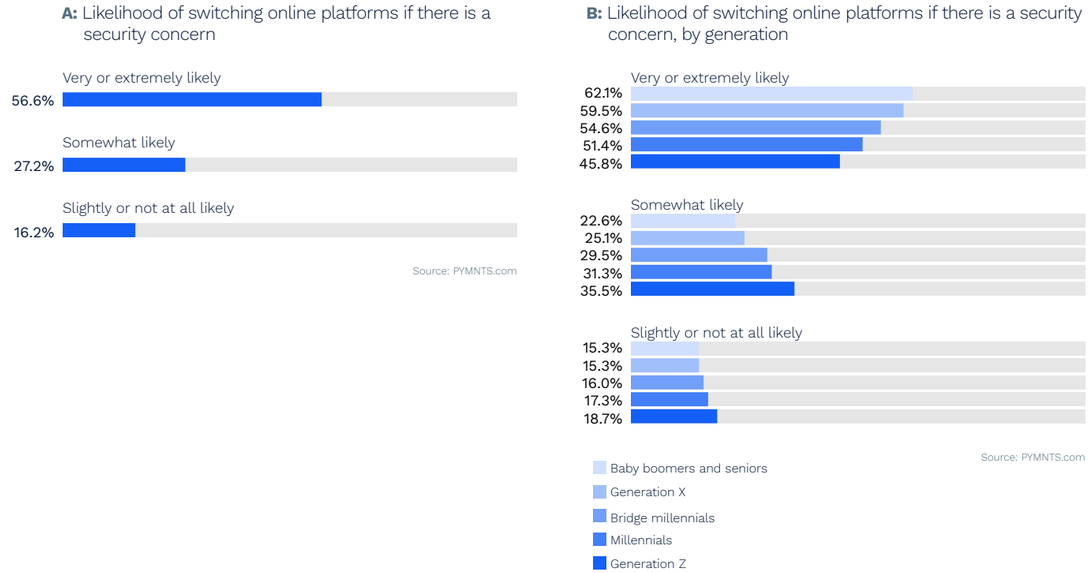
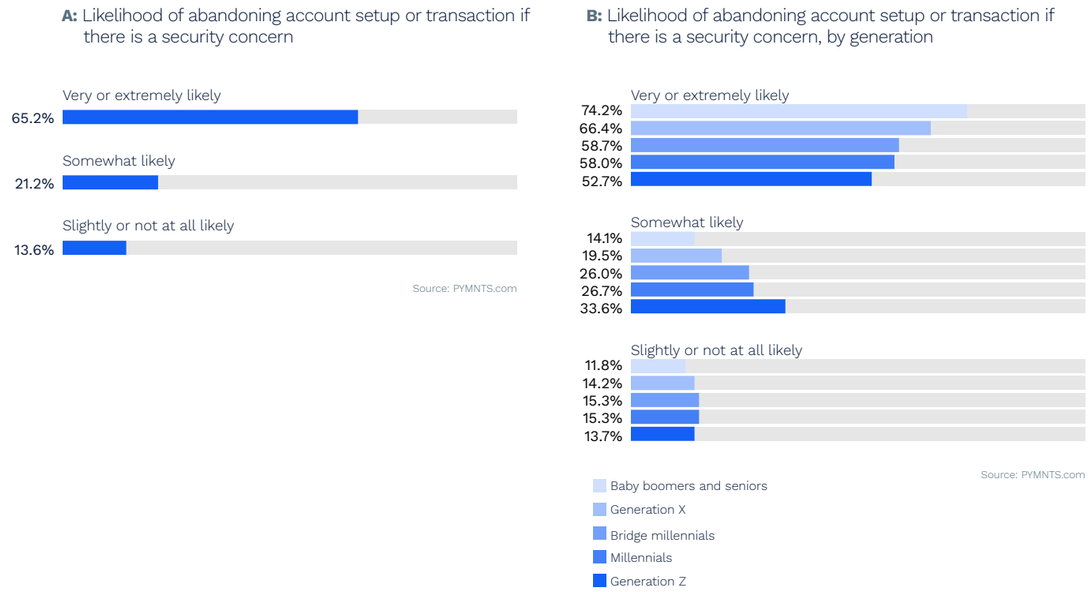


FIGURE 8: How concern about a platform not protecting or sharing PII can trigger abandonment

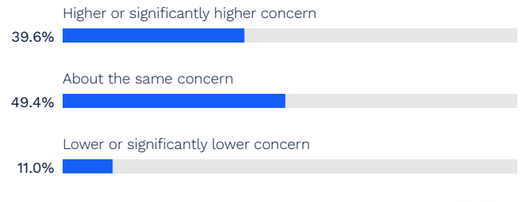


The new “data minders”

The security of PII matters to 94 percent of consumers, and four out of 10 are now more worried about the data security practices of merchants than they were a year ago. Some of these consumers’ fears are specific, such as the concern that someone might gain access to their data and open new accounts in their names (held by 11 percent) or steal their money (12 percent). Other fears are more general, like the concern that bad actors will use consumer data in some indeterminate, harmful way (held by 27 percent). Only 11 percent of consumers feel more confident that their data is safe than they did a year ago. The new “data minders” are motivated in their choice of merchant or platform by their sense of security about the way their personal details, including their payment credentials, are protected. Baby boomers and seniors are the most concerned about their data being accessed without their authorization (a 32 percent share held this worry), and Generation Z consumers are worried in the greatest shares about their information being tracked online (19 percent).

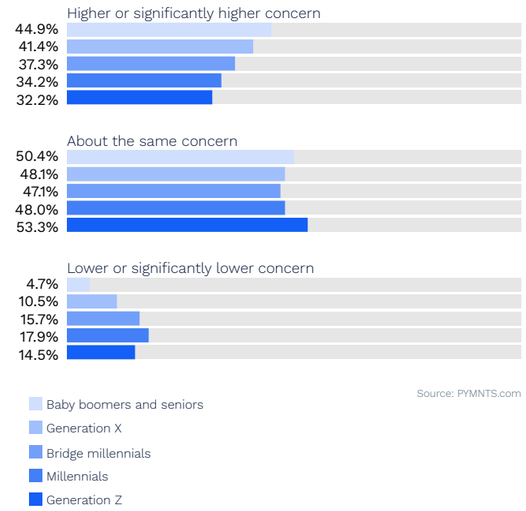
FIGURE 9: Evolution of concerns amongst consumers

A: Change in the level of concern



Source: PYMNTS.com

B: Change in the level of concern, by generation



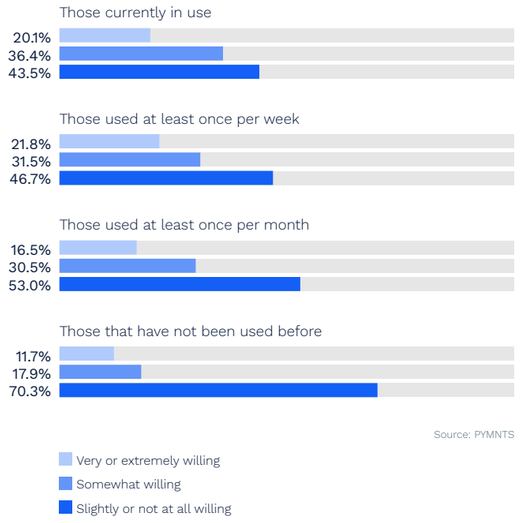
Source: PYMNTS.com

An honest (inter)face: Consumers tend to trust online retailers that they know well with their personal data.

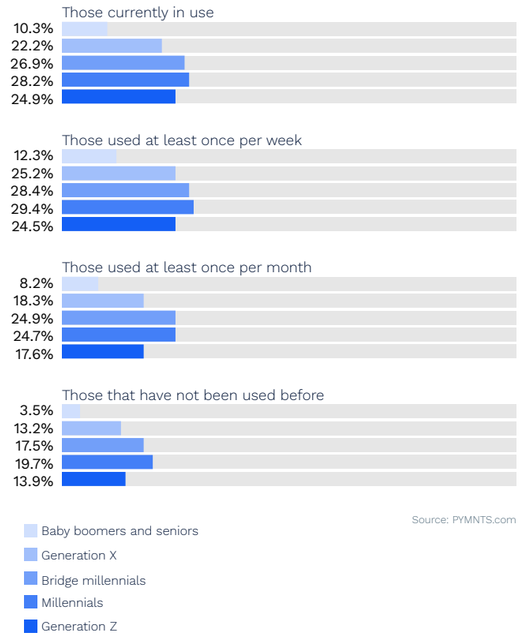
Most consumers are willing to share their data with digital platforms that they patronize frequently, and younger consumers are the most likely to store their personal data with a platform. Familiarity inspires trust online. Fifty-six percent of consumers are at least “somewhat” willing to provide PII to online platforms they currently use, and 20 percent are “very” or “extremely” willing to do so.

FIGURE 10: Consumers’ inclination to provide PII to select online platforms

A: Level of consumer willingness to provide PII to select online platforms



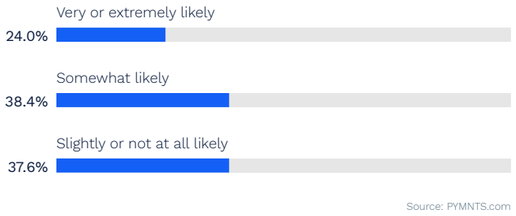
B: Share of consumers who are “very” or “extremely” willing to provide PII to select online platforms, by generation



PYMNTS’ researchers learned that platforms may exude trustworthiness by actively promoting their commitment to data security. Our data revealed that 62 percent of consumers are at least “somewhat” likely to provide PII if online platforms assure them that their data will be protected and not shared. Twenty-four percent are “very” or “extremely” likely to provide this data in this instance, and that share rises to 30 percent for Gen X and millennial consumers and 31 percent for bridge millennials. Online platforms’ assurances that their data is protected and not shared with third parties are “very” or “extremely” important for nearly three-quarters of consumers. These statements are important to baby boomers and seniors (83 percent agreed with this sentiment) and they also hold sway with more than half of Gen Z consumers (54 percent).

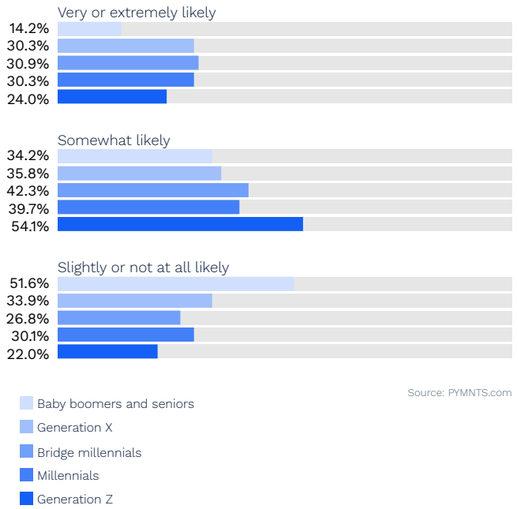
FIGURE 11: Assurances' impact on consumers' comfort providing PII

A: Consumers' likelihood of providing PII if an online platform provides assurances that data will be protected and not shared with third parties

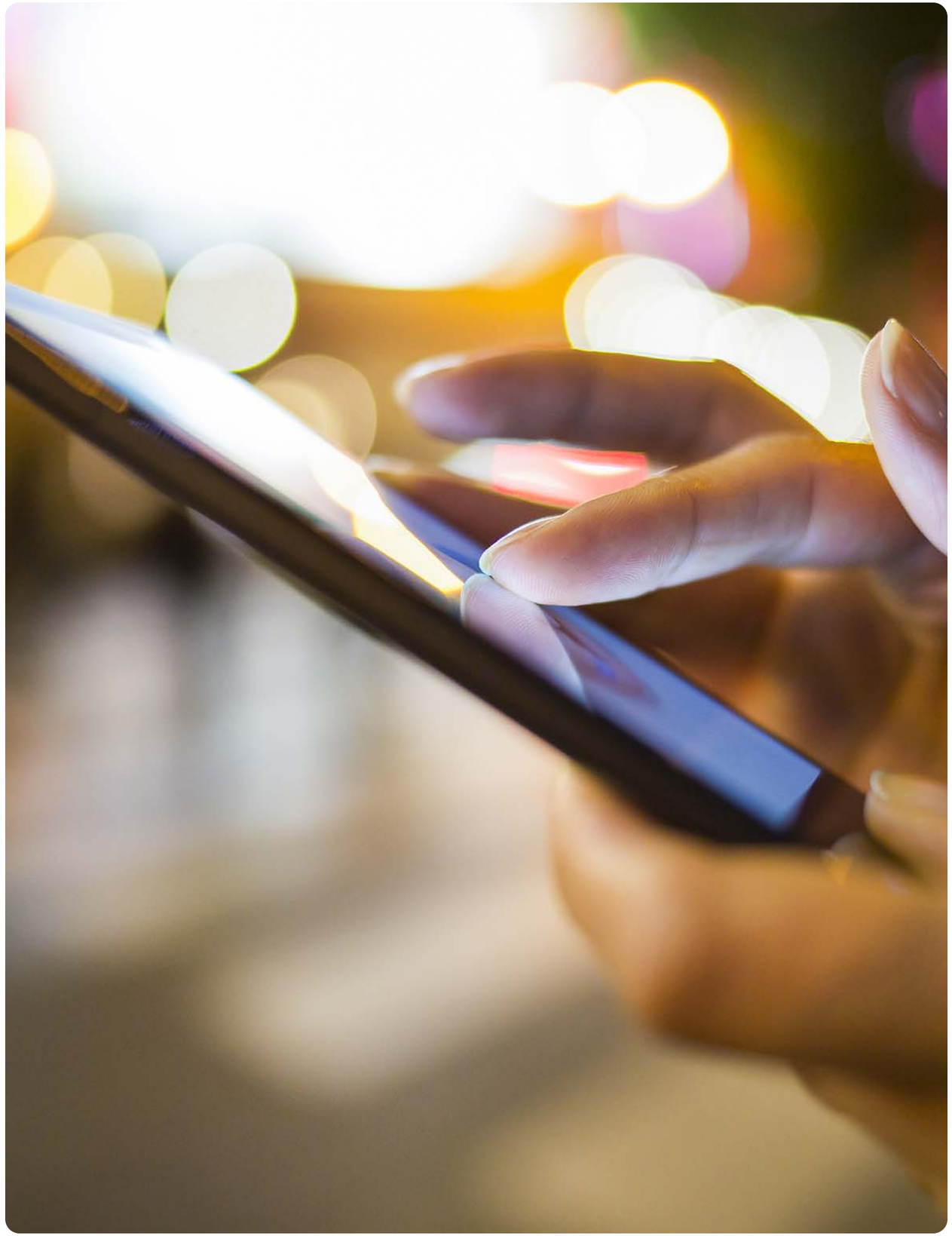


Source: PYMNTS.com

B: Consumers' likelihood of providing PII if an online platform provides assurances that data will be protected and not shared with third parties, by generation



Source: PYMNTS.com



Conclusion

As consumers interact with digital channels with greater frequency, their exposure to new types of digital risk may increase alongside their concern over their data's safety. Merchants receiving a flood of new online consumers and increasingly complex cybersecurity risks must be mindful of the importance of strong security on the back ends of their eCommerce operations, apps and other platforms. PYMNTS' research has found that consumers not only want to feel safe when shopping but also want assurances that their data is safe from the onboarding experience to the final transaction. Our data reveals that consumers may leave a platform at any time if they feel that their PII may be at risk. The challenge for merchants in the future will be to make consumers aware of the steps being taken to protect their data and make them trust that those measures are working for their benefit.

Methodology

The Privacy Paradox: Securing Data To Build Customer Engagement is based on a census-balanced survey of 2,257 U.S. consumers conducted from May 7 to May 13, 2021. The survey consisted of 13 questions concerning consumers' online shopping behaviors and their attitudes toward privacy, data security and related matters.

ABOUT

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.

VERY GOOD SECURITY

Providing essential security and compliance infrastructure, Very Good Security (VGS) enables startups and enterprises to focus on their core business instead of compliance and regulatory overhead. With one single integration, VGS customers unlock the value of sensitive data without the cost and liability of securing it themselves, while also accelerating compliances like PCI, SOC 2, GDPR and more.

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

The Privacy Paradox: Securing Data To Build Customer Engagement 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.