FINANCIAL HEALTH NETWORK

Financial Data

THE CONSUMER PERSPECTIVE

AUTHORS

Dan Murphy
Policy Manager

David Silberman
Senior Advisor

Stephen Arves
Manager

ACKNOWLEDGMENTS

Financial Data: The Consumer Perspective was prepared by Dan Murphy, David Silberman, and Stephen Arves of the Financial Health Network using data collected from surveys fielded using NORC at the University of Chicago's AmeriSpeak® Panel. The authors would like to thank Suzanne Howard, Stefan Subias, and Mark Watts from NORC at the University of Chicago for their commitment to this work, as well as Kaitlin Asrow, Corey Stone, and Chuck Muckenfuss for their feedback on the survey instrument. The authors would also like to extend a special thanks to Linda Jeng of Georgetown University and Transparent Financial Systems, who was an invaluable early thought partner on this work.

Contents

Definitions

Application programming interface (API): An API is an intelligent conduit that allows for the flow of data between systems in a controlled yet seamless fashion.[1] Many data holders (such as banks) have established their own APIs to share customer data with third parties.

Data aggregator: Data aggregators are technology companies that facilitate the transfer of financial data. While data aggregators sometimes transfer data for internal use by data holders (such as banks), this report focuses on transfers at the direction of consumers who want to move their data from data holders to nonaffiliated financial services providers (such as fintech apps).

Data minimization: Data minimization refers to the practice of collecting only the minimum amount of data required for application functionality and storing that data only for the minimum amount of time needed.[2]

Data portability: Data portability refers to the ability of consumers to take their data from a service or institution and transfer, or port, it elsewhere.[3]

Section 1033 of the Dodd-Frank Act: Section 1033 of the Dodd-Frank Act states that, subject to rules prescribed by the Consumer Financial Protection Bureau (CFPB), covered financial institutions and their affiliated service providers must make certain consumer financial information available to consumers in electronic form. The CFPB recently issued a notice of its intent to undertake a rule-making to affirm consumers' right to access their data under Section 1033.[4]

Fintech app: For the purposes of this report, "fintech apps" include apps that link to a consumer's primary checking account, credit cards, or investment accounts to help them manage their money or enable them to make payments (such as Mint, Venmo, and Digit). This survey specified that fintech apps do not include the mobile banking apps offered by a consumer's primary financial institution.

Gramm-Leach-Bliley Act (GLBA): Among numerous other provisions, GLBA broadly states that a financial institution has "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." The two substantive areas of GLBA addressing financial data have become known as the Privacy Rule, which regulates when and how financial institutions are permitted to share consumers' personal data, and the Safeguards Rule, which requires financial institutions to take steps to protect the confidentiality and security of customer data from unauthorized access.[5]

Online lender: For the purposes of this survey, online lenders were broadly defined as companies that make loans online (such as Rocket Mortgage from Quicken, SoFi, and Prosper).

Opt-in standard: A consent standard that requires individuals to specifically and affirmatively consent to a specified activity.[6]

Opt-out standard: A consent standard in which individuals are given the opportunity to indicate their preference not to take part in a specified activity.[7]

Personal data: For the purposes of this survey, "personal data" was broadly defined to be inclusive of information consumers are required to give a bank or credit union when opening a checking account (such as their email address and Social Security number), as well as financial information (such as deposits, checks, and bill payments).

Primary financial institution (PFI): For the purposes of this report, a consumer's primary financial institution is defined as the bank or credit union that houses the consumer's primary checking account.

Screen-scraping: Screen-scraping is the automated, programmatic use of a website, impersonating a web browser, to extract data or perform actions that users would usually perform manually on the website.[8] In the financial data ecosystem, some data aggregators access consumers' accounts with login credentials provided by the consumer and then use screen-scraping to capture the data they need to transfer to a fintech app or other third party.

[1] *Laura Brodsky & Liz Oakes, "Data sharing and open banking," McKinsey & Company, September 2017.*

[2] *Kaitlin Asrow & Beth Brockland, "CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration," Financial Health Network, October 2016.*

[3] *Bennett Cyphers, Gennie Gebhart, & Kurt Opsahl, "What We Mean When We Say 'Data Portability'," Electronic Frontier Foundation, September 2018.*

[4] *"Consumer Financial Data: Legal and Regulatory Landscape," Financial Health Network, FinRegLab, Flourish, & Mitchell Sandler LLC, October 2020.*

[5] *Ibid.*

[6] *Donna Gillin, "The Opt-in vs. Opt-out Debate," The Insights Association, February 2001. Where hyphenated, "opt-in" denotes adjective form.*

[7] *Ibid. Where hyphenated, "opt-out" denotes adjective form.*

[8] *"Screen scraping 101: Who, What, Where, When?," The Open Banking Hub, July 2017.*

Executive Summary

In recent years, technology has changed the way that consumers interact with financial services providers, making digital channels the hub of consumers' financial lives.

This transition has given rise to new types of financial products, services, and institutions, and has the potential to deliver significant benefits to consumers. However, this new paradigm comes along with an increase in the availability of consumer financial data, bringing new risks for consumers, financial institutions, and policymakers to consider. As in other sectors, consumer understanding and views of the use of personal data are evolving.

In this report, the Financial Health Network describes the results of a nationally representative survey that was fielded to uncover consumer understanding and viewpoints on current practices in the financial data ecosystem. The report describes consumer understanding of how banks and credit unions, technology companies, fintech apps, and data aggregators treat data about consumers, and consumer preferences on how they would like personal data to be treated.

Our analysis finds that overwhelming majorities of consumers favor data minimization, prefer that data about them not be shared for marketing purposes, and prefer that financial institutions operate under an opt-in standard for data sharing. We also find that a majority of consumers believe their bank should be required to share personal data if they ask it to do so.

The Financial Health Network hopes these results can serve as a guide to both industry stakeholders and policymakers who seek to build trust and ensure that both practice and policy serve consumers.

Methodology

The data for this report were collected from surveys fielded using NORC at the University of Chicago's AmeriSpeak® Panel, a randomly selected probability-based internet and phone panel. It includes a general population sample of U.S. adults ages 18 and older, and the survey was limited to those within the panel who have a personal checking account with a bank or credit union. In total, NORC collected 2,037 interviews between Jan. 15 and 29, 2021.[9] We applied post-stratification weights to the full sample to make it nationally representative with respect to age, gender, census division, race/ethnicity, education, housing tenure, and household phone status. Refer to the Appendix for additional information on the Methodology and the AmeriSpeak® Panel.

Note that figure percentages may not total 100 because of rounding, a small number of nonresponses, or both.

[9] NORC collected 2,026 by web mode and 11 by phone mode.

Our Findings

KEY FINDING 1 62% of consumers think their bank should be required to share data about them if they direct it to.

KEY FINDING 2 90% Approximately 90% of consumers favor an opt-in standard for banks, tech companies, and fintech apps to share data about them.

KEY FINDING 3 87% of consumers favor data minimization, but only 41% think it is taking place in the market today.

KEY FINDING 4 Consumers' views on data portability, data minimization, and opt-in standards do not vary with political party affiliation.

68% of consumers have linked financial applications to their checking account.

93% of fintech app users and borrowers aren't aware of data aggregators' presence in their financial lives.

90% Approximately 90% of consumers prefer that banks, tech companies, and fintech apps not share data about them for marketing purposes.

Introduction

Americans' attitudes about the use of personal data are evolving.[10] A decade ago, technology companies using data about their customers enjoyed broad popularity and a high degree of trust for offering useful (and often free) products and services that connected people in new ways and generally made their lives more convenient. While some privacy advocates raised alarms, a commonly heard sentiment among Americans was "I have nothing to hide." Today, that has begun to change.[11]

The popularity of technology companies has been greatly damaged by stories of data breaches, targeted misinformation campaigns, and a wide range of egregious violations of individual privacy. Some of those who previously felt they had nothing to hide may have begun to feel less like a consumer, and more like a product.

While this debate over technology companies and new forms of data has taken center stage, there have also been significant developments in the financial services sector. As in other sectors, innovative firms have found new ways to use personal data. Many of these uses hold the potential to produce significant benefits for consumers and financial institutions alike. Unlike in some other sectors, however, the use of consumer financial data is governed by a number of consumer protections at the federal level. Still, these protections were not created with today's financial data ecosystem in mind, and the limitations they create are often anachronistic, vague, or subject to so many exceptions that they are rendered impotent.[12]

Importantly, there has been comparatively little research into consumers' understanding and viewpoints on current practices in the financial data ecosystem in the United States. Some surveys have explored consumers' feelings on data privacy more broadly and have even indicated that consumers consider financial information to be particularly sensitive, but few have gone deeper in the financial services sector.[13] Conversely, much research that does go deeper in financial services tends to pay more attention to consumer trust than to specific attitudes on data portability, data minimization, or opt-in/opt-out standards, for example.[14] While this research confirms that consumers care about privacy but are relatively unlikely to change their banking relationships, it tells us less about their understanding of the financial data ecosystem's nuances. Some trade groups and individual companies have published research that focuses on such questions in financial services, but these may suffer from perceptions of bias.[15]

In order to ensure that consumers' views are considered as the financial services industry continues to innovate and policymakers revisit appropriate consumer protections, the Financial Health Network fielded a nationally representative survey to uncover consumer understanding and viewpoints on current practices in the financial data ecosystem. In this report, we describe the results of that survey, which we hope can contribute to the debate and inform both industry stakeholders and policymakers who seek to build trust and ensure that both practice and policy serve consumers.

[10] Mike Allen & Ina Fried, "Exclusive: Trust in tech craters," Axios, March 2021; "Edelman Trust Barometer 2021," Edelman, March 2021.

[11] Monica Anderson, Brooke Auxier, Madhu Kumar, Andrew Perrin, Lee Rainie, & Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, November 2019.

[12] "Consumer Financial Data: Legal and Regulatory Landscape," Financial Health Network, FinRegLab, Flourish, & Mitchell Sandler LLC, October 2020.

[13] "Data privacy: What the consumer really thinks," The Data & Marketing Association and Acxiom, June 2018.

[14] "Trust in Financial Services," Morning Consult, May 2021.

[15] "Consumer Survey: Financial Apps and Data Privacy," The Clearing House, November 2019; Matthew Homer, "Plaid Policy Pulse: greater control for consumers," Plaid, June 2019.

The Financial Health Connection

Consumer data create a foundation for financial innovation, a challenge for consumer protection, and an opportunity to foster competition.

Financial Innovation	By using consumer data creatively, innovative firms are able to offer new kinds of products and services and expand access to existing products and services in ways that can support financial health, including by making credit more accessible and affordable and by giving consumers greater control of their financial lives.
Consumer Protection	While consumer data are broadly available for consumers to share, many questions remain with respect to reliability, consent, security, minimization, and privacy.[16]
Competition	Access to financial data can help lower barriers to entry in financial services, allowing new entrants to design financial health-focused products and services.[17]

[16] *Dan Murphy, "Testimonial: CFPB Consumer Access to Financial Records Symposium," Financial Health Network, February 2020; Dan Murphy, "Comment Letter: Consumer Access to Financial Records," Financial Health Network, February 2021.*

[17] *Dan Murphy, "Comment Letter: CFPB Taskforce on Consumer Financial Law," Financial Health Network, June 2020.*

Primary Financial Institutions

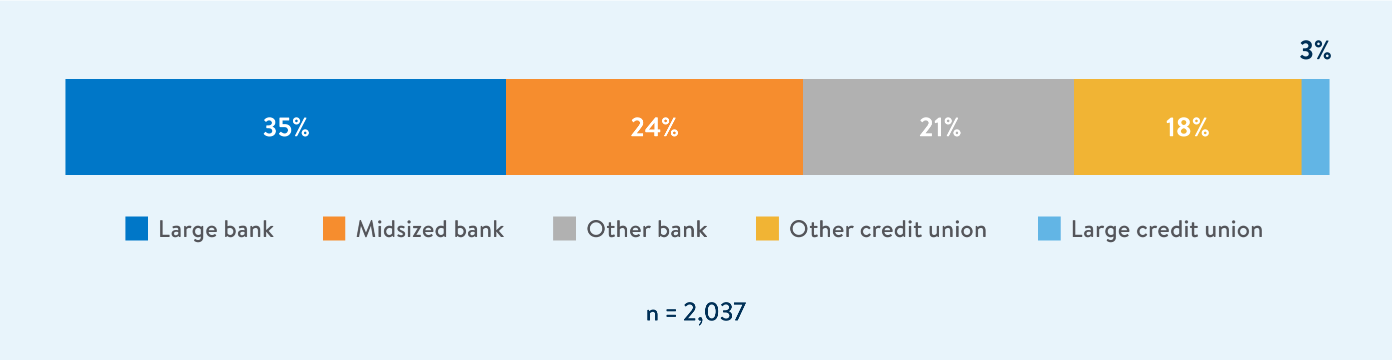
According to the most recent survey conducted by the Federal Deposit Insurance Corporation (FDIC), approximately 95% of Americans have a checking account at a bank or credit union.[18] This makes banks and credit unions the primary financial institution (PFI) for most consumers. Likewise, checking accounts are the most commonly held financial product and the one where Americans are most likely to have a shared experience of how financial institutions treat their data. In this section, we present findings that pertain to checking accounts at consumers' banks and credit unions, referred to as their PFI.

Americans' checking accounts are housed at banks and credit unions of differing sizes and characteristics, and consumers may have vastly different experiences.

While banks and credit unions offering checking accounts are bound by a similar set of laws and regulations that govern how they may use consumer data, research has shown that even similar institutions' stated practices can vary widely.[19]

Financial institutions' practices are described in a privacy policy disclosure provided to consumers when they open an account and periodically thereafter, as set out by the Gramm-Leach-Bliley Act (GLBA). Consumers' understanding of the use of their data greatly depends upon their receiving, reading, and understanding these privacy policies, but there is growing evidence that consumers are overwhelmed by the number of privacy policies in their lives and have given up trying to engage with and understand them.[20]

Figure 1. Types of primary financial institutions (PFIs).[21]



[18] "How America Banks: Household Use of Banking and Financial Services," FDIC, October 2020.

[19] Lorrie Cranor, Pedro Leon, & Blase Ur, "A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices," 2016.

[20] Kaitlin Asrow, "The Role of Individuals in the Data Ecosystem," Federal Reserve Bank of San Francisco, 2020.

[21] Large banks are Bank of America, Wells Fargo, JPMorgan Chase, and Citibank. Midsized banks are US Bank, PNC, TD Bank, Capital One, USAA Bank, Citizens, BB&T, SunTrust, Fifth Third, Huntington, KeyBank, Regions, Discover Bank, TCF, and Truist. Other banks consist of "another bank not listed." Other credit unions consist of "another credit union not listed." Large credit unions are Navy Federal Credit Union, State Employees' Credit Union, Pentagon Federal Credit Union, and BECU. As noted in the Methodology section, figure percentages may not total 100 because of rounding, a small number of nonresponses, or both.

According to our analysis, approximately 1 in 5 consumers report that they either did not receive or do not recall receiving their PFI's privacy policy. Among the 81% of consumers who did recall receiving the privacy policy, 79% reported either not reading or merely skimming it.

Put another way, only 16% of consumers report having read most or all of their PFI's privacy policy.

Not surprisingly, our analysis also indicates that consumers have limited understanding of their PFI's privacy policies, with over half reporting that they don't know whether their PFI's privacy policy allows it to give other companies access to data about them. Further, despite GLBA's requirement that financial institutions notify and provide consumers with a way to opt out of certain data sharing, only about 1 in 4 consumers reports having exercised their right to do so. As low as that is, it may actually overestimate the extent to which consumers act on privacy disclosures, as industry estimates suggest that only 5% of consumers opt out of optional data sharing.[22]

Figure 2. Receipt and use of privacy policies from PFIs.

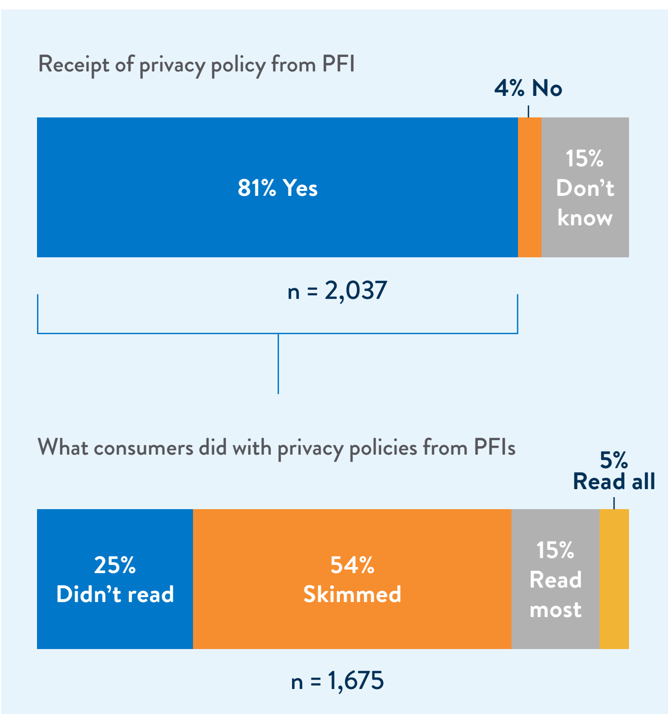
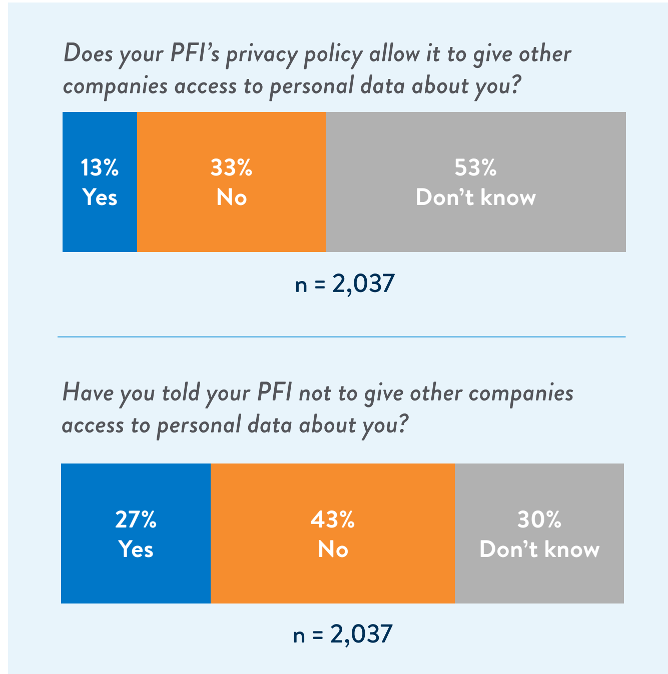


Figure 3. Awareness of data sharing policies and frequency of opt-out use at PFI.

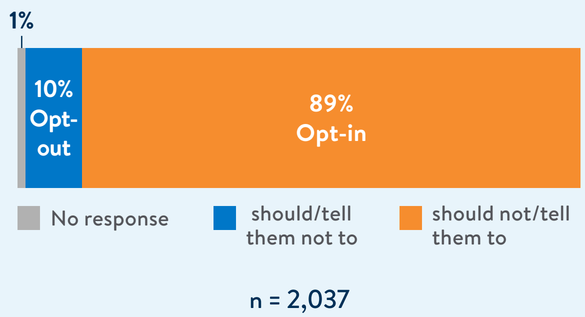


Despite the limited number of consumers who reported exercising their right to opt out of optional data sharing, consumers also expressed an overwhelming preference (94%) for their PFI not to share data about them with other companies for marketing purposes. When asked whether they would prefer an opt-out or opt-in standard for such data sharing, a similarly overwhelming majority (89%) of consumers stated that they would prefer that financial institutions' data sharing be bound by an opt-in standard.

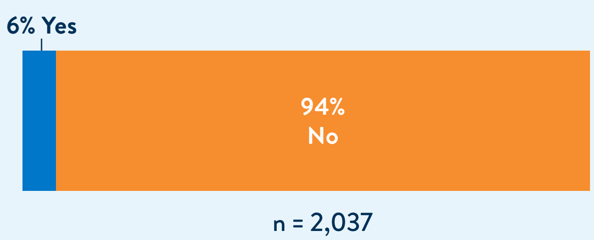
[22] "Opt-Out Notices Give No One a Thrill," *American Banker*, July 2001.

Figure 4. Consumers prefer opt-in standards and less data sharing by their PFI.

Which of the following most closely describes your opinion? It ______ be legal for your current bank or credit union to give other companies access to personal data about you, unless you ______ .



Would you like your current bank or credit union to give other companies access to personal data about you so they can market products and services to you?

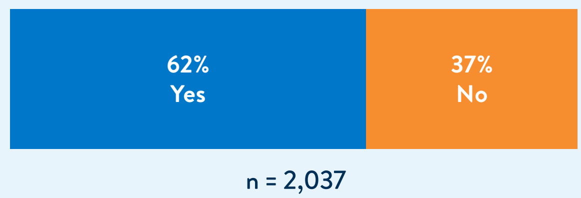


Despite the vast majority of consumers' apparent discomfort with data sharing directed by a financial institution itself, our analysis indicates that many of those same consumers feel differently about data sharing that they themselves have directed (often referred to as data portability). Over 60% of consumers indicated that they believe their financial institutions should be required to share their personal data with another company (such as a fintech provider) if the consumer directs them to do so.

Our analysis also indicates that these preferences hold across demographic groups, including age, gender, education, race/ethnicity, and household income. Even among self-identified Republicans and Democrats, similarly strong majorities are in lockstep on their strong dislike of data sharing for marketing purposes, their overwhelming preference for an opt-in standard, and their belief that their PFI should be compelled to share their personal data if they direct it to.[23]

Figure 5. The majority of consumers believe they should have the right to data portability.

If you ask your current primary bank or credit union to give another company personal data about you from your account, should your bank be required to do so?



[23] *This is discussed in greater detail in the Synthesis section.*

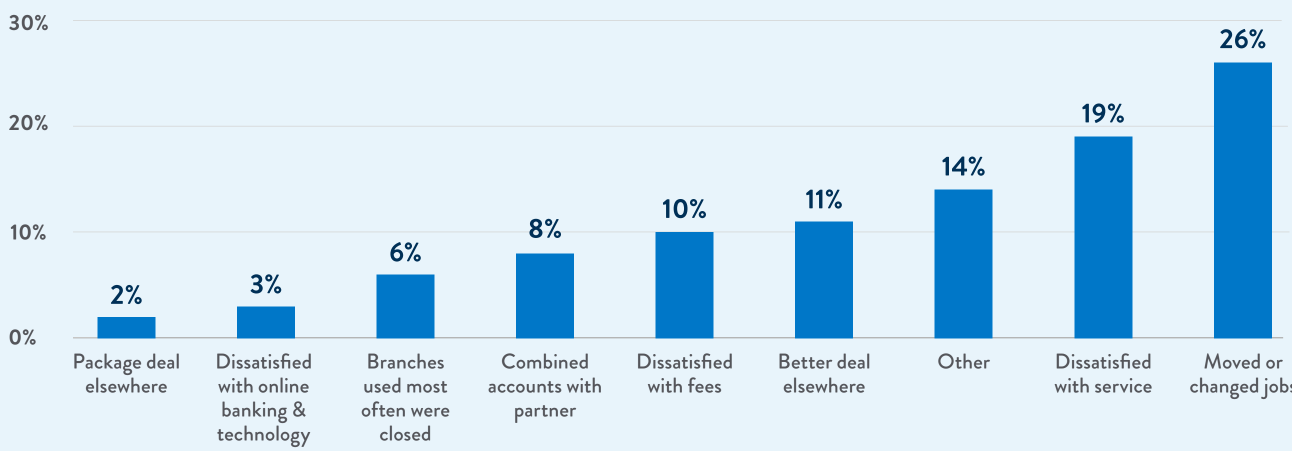
Bank Switching

As fintech providers increase their foothold in financial services, one of the benefits policymakers hope they bring is an increase in competition. Many fintechs have called for an affirmation of consumers' right to data portability under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which they argue will enable innovation that helps them compete with incumbent banks and credit unions. However, while data portability may do much to bring new entrants to financial services or enable the development of new products, it does less to encourage competition between existing financial service providers offering similar products, for example.

Consumers switch their financial services provider so infrequently that it is often said that consumers switch life partners more often than they switch their bank. Our analysis indicates that 70% of consumers have had their current PFI for more than five years, and almost 40% have had it for more than 15 years. Among those who have had their PFI for five years or less, only 20% report having a previous PFI.

This inertia does little to incentivize PFIs to take steps to maximize their customers' financial health. Among those few who have switched PFIs, it was more common to do so because of moving or changing jobs, rather than dissatisfaction or finding a better deal elsewhere.

Figure 6. Primary reasons for switching PFIs. (n = 456)[24]



Many believe these low switching rates are the result of friction from the need to switch direct deposit and bill pay whenever one changes their PFI. To lessen this friction, some fintechs have begun to enable direct deposit switching. Other observers believe we need to go further, and have called for full "account number portability" to increase competition between PFIs.

However, if low switching rates are the result of such friction, our analysis did not uncover it. Among consumers who have switched PFIs, 70% said it was easy or very easy, and consumers tended to give their PFIs high Net Promoter Scores. While these data are limited, they may indicate that reducing friction to enable bank switching would have only a marginal effect on consumer inertia.

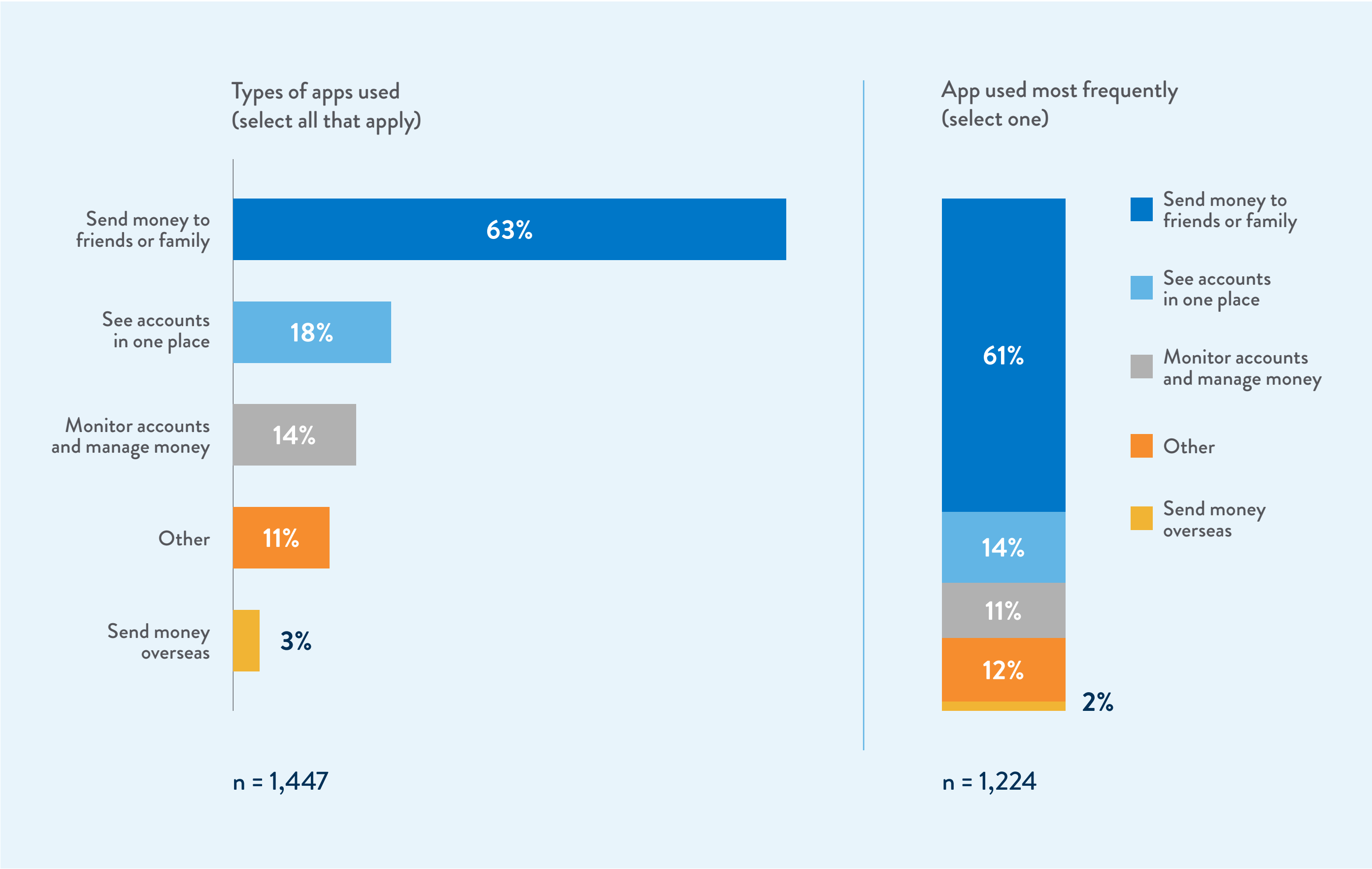
[24] *Only survey participants who had been with their PFI for less than five years and also indicated that they previously had a primary checking account with a different bank or credit union answered this question.*

Financial Technology Providers

Consumer perspectives on data portability are particularly relevant today, as a large number of nonbank financial technology providers (fintechs) have emerged to provide consumers with new types of financial products. To offer their products, fintechs often require access to consumer data housed at the consumer's PFI. This data use may enable fintechs to offer products that promote consumer financial health, but it also adds a layer of complexity to a financial data ecosystem that consumers already struggle to understand. In this section, we present findings that pertain to these relatively new types of entities and use cases.

While fintech usage is less common than checking account usage, our analysis found that 68% of consumers with checking accounts have linked nonbank fintech apps to their checking account. Among fintech users, apps used to send money to friends or family were used by the majority of respondents, and were also identified as the type of app that consumers used the most often.

Figure 7. Types of fintech apps used and apps used most frequently.



When consumers sign up to use a fintech app, they often need to link the app to their checking account to ensure the app has the data it needs to perform its core function. For an app used to send money, for example, this connection allows the app to confirm that a consumer has sufficient funds to complete the transaction. For a personal financial management app that helps consumers manage cash flow, anticipate expenses, or avoid overdrafts and bounced payments, this connection may provide a constant stream of data that updates a consumer's checking account or credit card balance as the consumer makes purchases, gets paid, and makes other withdrawals and deposits.

To initiate and maintain this link to consumer accounts, fintech apps often use third-party service providers, referred to as data aggregators. Data aggregators help the fintech app connect and stay connected to a consumer's account and aim to ensure a seamless experience on the fintech app for the consumer. However, the presence of data aggregators and the scope of their access to data about a consumer may not always be apparent to consumers, unless they have carefully read and understood privacy policies and other disclosures they might have been shown when downloading a fintech app or linking it to their PFI account. In fact, we found that only 7% of consumers who have linked a fintech app or an online lender to their PFI account recall being linked to a data aggregator.

Whether or not consumers are aware of a data aggregator's presence, most fintech app users and online borrowers who link their PFI account to a fintech app or lender would have done so through a data aggregator. Typically, these consumers provide some type of identifying information to verify their identity. In some cases, they may provide the username and password for their online banking account to the fintech app or data aggregator, which uses it to log into their bank on their behalf and collect, or screen-scrape, some or all of the data that would be available to the consumer if they logged in themselves. In other cases, the consumer may be redirected from the fintech app interface to their PFI's online banking portal, where they log in using their credentials and provide consent for their bank to share data with the fintech app or lender through an application programming interface (API) or agreed-upon screen-scraping arrangement. In still other cases, a consumer may provide their account and routing numbers, or their credit card number, to aggregators or directly to the fintech app. According to our findings, fintech app users are almost evenly split between those who remember giving their username and password, those who remember giving other identifying information, and those who don't remember which information they gave.

Figure 8. Fintech app users and online borrowers who were directed to a data aggregator.

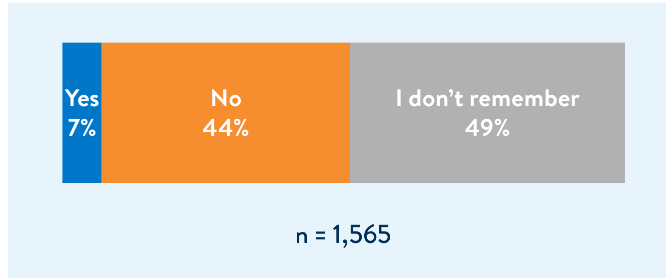
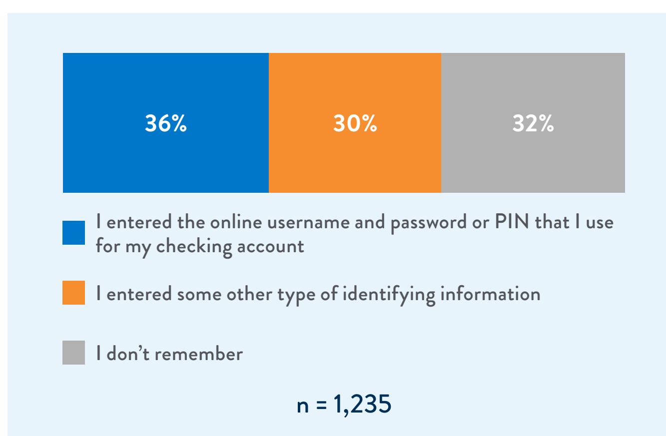
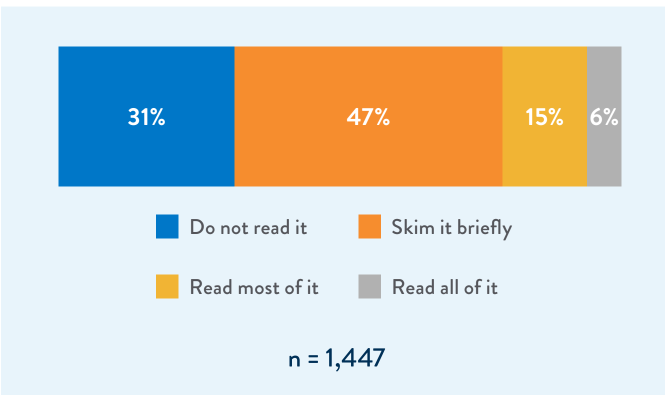


Figure 9. How fintech app users linked their fintech app to their PFI account.



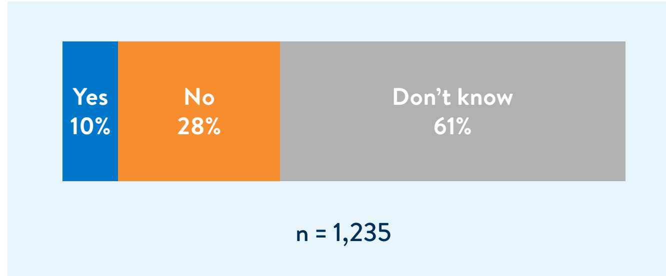
Often, when a consumer signs up with a fintech app or connects the app to their PFI account, they are shown or offered a link to a privacy policy that describes how their personal data will be used. Receiving, reading, and understanding these privacy policies is critical for consumers to understand the use of data about them, but as noted, many consumers are overwhelmed by the number of disclosures they receive and have given up on reading each of them closely. According to our analysis, almost 80% of consumers either did not read or merely skimmed the privacy policy provided when signing up with their fintech app or linking it to their PFI account.

Figure 10. What fintech app users do with the privacy policies they are provided.



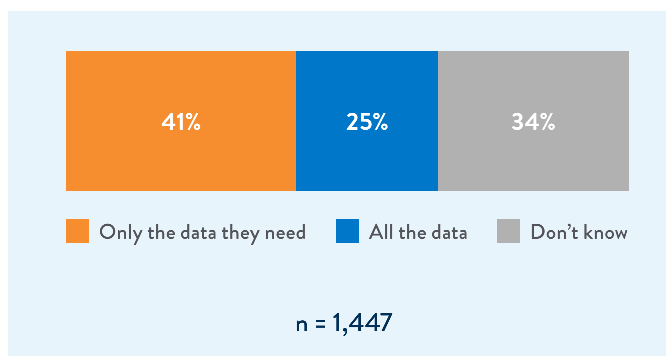
Unsurprisingly, this lack of engagement with fintech apps' privacy policies makes it difficult for consumers to understand what those policies imply for the use of data about them. According to our analysis, 61% of fintech app users do not know whether their fintech app's privacy policy allows the fintech app to give other companies access to information about them. Moreover, even among those who report having read most or all of their fintech app's privacy policy, 35% indicated that they do not know whether the privacy policy allows the fintech app to give other companies access to information about them.

Figure 11. Does your fintech's privacy policy allow it to share your data with other companies?



This lack of understanding applies not only to consumers' understanding of whether or not their fintech app can share consumer data with other companies, but also to their understanding of how much of their checking account data their fintech app is able to access itself. When asked how much of their checking account data their fintech app is able to access, 41% reported understanding that it could only access the data it needed (a practice referred to as data minimization), 25% reported understanding that it could access all of their data, and 34% reported that they did not know. While it is difficult to assess how closely these perceptions match market activity, the prevalence of the credential-sharing and screen-scraping methods used by some of the largest data aggregators in the market raises doubts.[25]

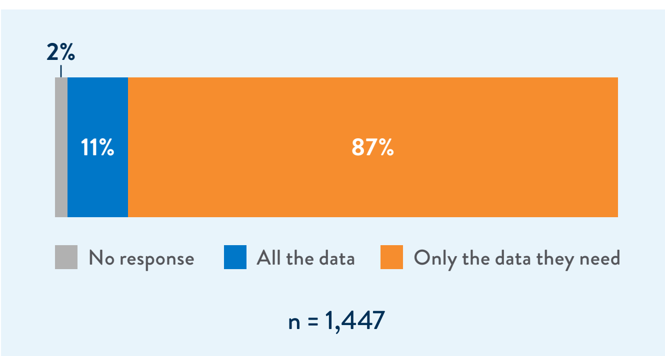
Figure 12. How much of your checking account data are fintech apps capable of accessing?



[25] *According to a Visa presentation, the data aggregator Plaid provides connections for 80% of the largest U.S. fintech apps. While the number of Plaid connections maintained through credential sharing and screen-scraping is reportedly shrinking, many such connections are thought to remain, and it is known that other data aggregators use these methods as well.*

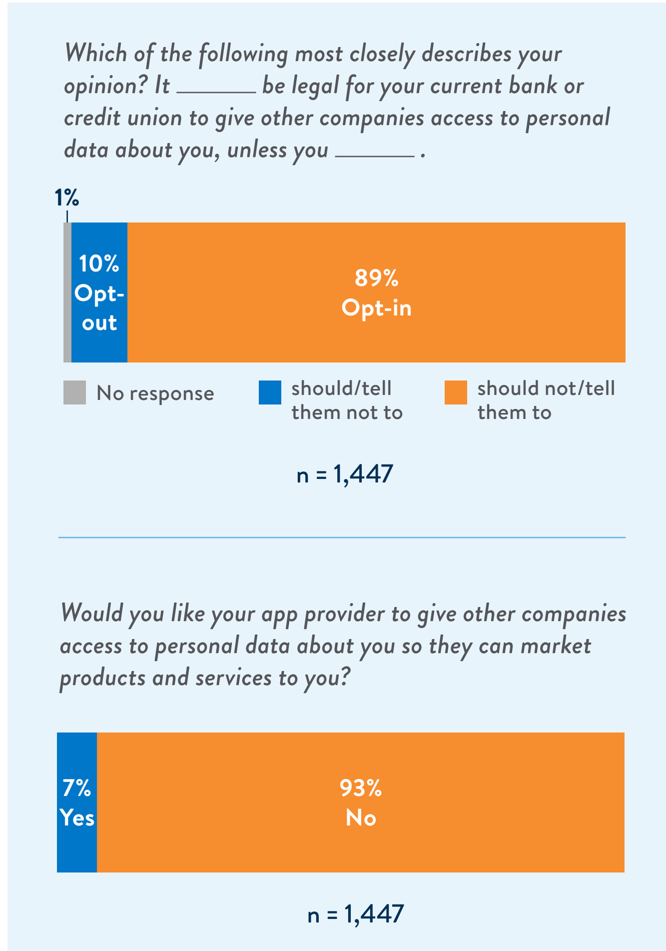
As is the case with PFIs, we found that despite consumers' limited understanding of current practices in the financial data ecosystem, they have an overwhelming preference for privacy. With respect to fintech apps, they also express an equally strong preference for data minimization that is out of step with their perception of the amount of data that fintech apps can access currently. While Figure 12 (above) shows that 59% of consumers either don't know how much data fintech apps are capable of accessing or think that fintech apps are capable of accessing all the data from their checking account, our findings show that 87% of consumers would prefer that fintech apps only be able to access the data they need from their checking account. Put another way, 87% of consumers favor data minimization, but only 41% of consumers think it is occurring in the market today – and even that 41% may overstate the extent to which data minimization actually is occurring.

Figure 13. How much checking account data fintech apps should be able to access.



Not unlike consumer sentiment with respect to their PFI, our analysis indicates an overwhelming preference for data sharing by fintech apps to be bound by an opt-in standard, and a similarly overwhelming preference for fintech apps not to share data about them for marketing purposes.

Figure 14. Consumers would prefer opt-in standards and less data sharing by fintech apps.



Synthesis

Having discussed consumer relationships with PFIs and fintech providers in isolation above, we will now describe the study's thematic findings. More specifically, this section looks at consumer experiences with privacy disclosures and data sharing policies across both types of institutions. Where possible, we compare these experiences to consumers' experiences with large technology companies, which are widely regarded as key players with respect to consumer data. We also look at whether prevailing attitudes vary with political party affiliation.

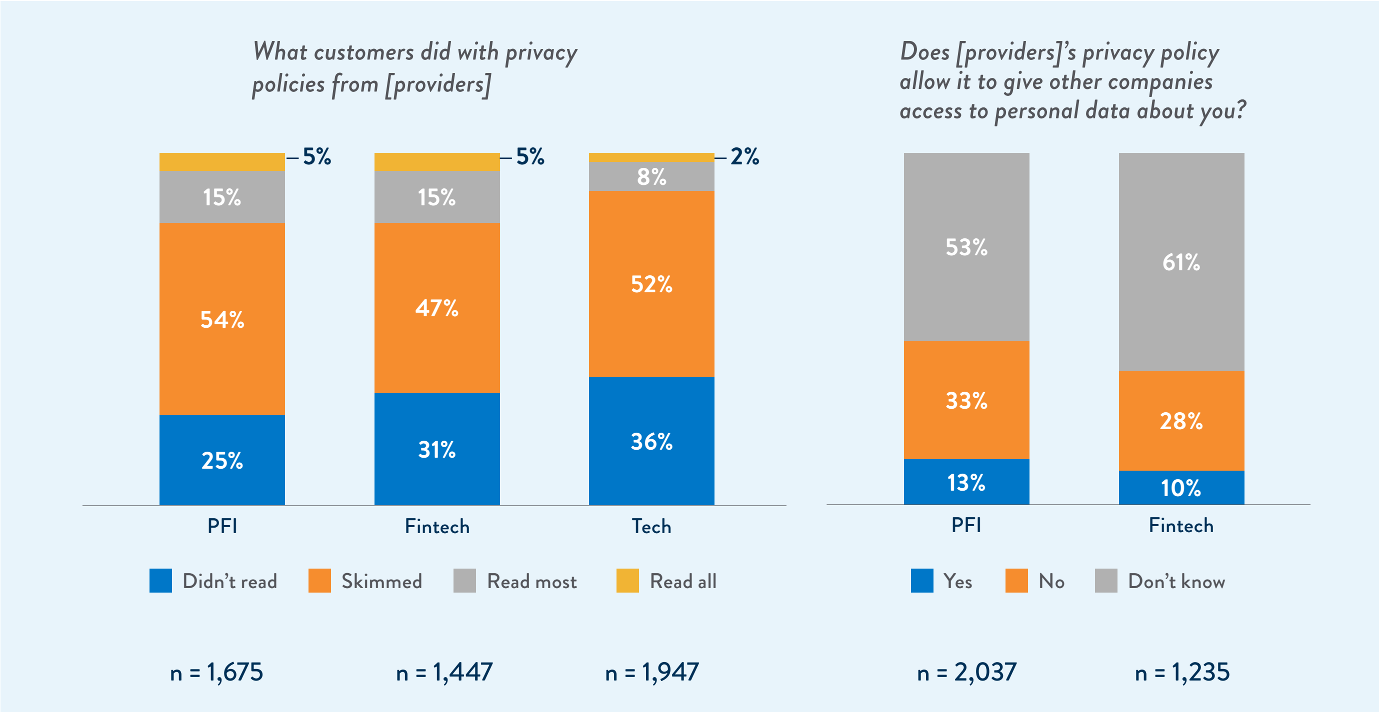
Privacy Disclosures

While it should not come as a surprise that consumers are unlikely to thoroughly read privacy policies, it is helpful to put our findings on PFIs and fintech providers into context. Unlike many technology companies, for example, all PFIs and many fintech app providers are legally obligated under GLBA to provide consumers with a copy of their privacy policy when they open an account and periodically thereafter, if the policy changes. Many consumers receive these disclosures in the mail and think little of them, but even that is more engagement than they might have with the privacy policy of their preferred social media provider, search engine, or other technology company.

Our findings indicate that customers of institutions subject to GLBA may be somewhat more likely to read privacy policies than customers of institutions without such an obligation. However, even customers of institutions subject to GLBA remain overwhelmingly more likely to skim or not read the privacy policies provided by PFIs and fintech apps, as shown in the left panel of Figure 15.

However, reading a privacy policy does not necessarily translate to understanding it, as numerous studies indicate. As shown in the right panel of Figure 15, our findings also indicate that the majority of consumers reported not knowing whether either their PFI's or fintech app's privacy policies allow them to give other companies access to data about them.

Figure 15. Most consumers don't read disclosures thoroughly and don't know what they allow.[26]



Data Sharing

Despite slight differences in consumer engagement with and understanding of privacy disclosures from PFIs, fintechs, and technology companies, consumers' perspectives on data sharing are unwavering across entities. Our analysis indicates an overwhelming preference for legally binding opt-in standards for data sharing and an even more overwhelming opposition to data sharing for marketing, as shown in Figure 16. This consistency is notable in light of other research findings that Americans trust technology companies more than financial institutions but look to financial institutions for leadership on data privacy.[27] Our findings show these perceptions do not affect how consumers would like their data to be treated.

Taken together with consumers' belief that their PFI should be compelled to share data about them if they direct it to (as shown in Figure 5) and their preference for data minimization (as shown in Figure 13), these results can be interpreted as a strong desire among consumers for greater control of personal data. While consumers reserve the right to direct data about them to be shared for a purpose they themselves have selected, they are simultaneously in favor of careful limitations to the scope of the data they share, a legal prohibition on data sharing they have not affirmatively opted in to, and a presumption that they do not want data about themselves shared for marketing purposes. These preferences are remarkably strong across the ideological spectrum, as shown in Figure 17. The preferences also hold across demographic groups, including age, gender, education, race/ethnicity, and household income (not shown).[28]

[26] *Note that the question referred to in the left panel was asked only of the 81% of PFI respondents who indicated that they remember receiving their PFI's privacy policy, while all fintech app and technology company users were asked this question. Because consumers of PFIs who do not recall receiving their PFI's privacy policy are unlikely to have read it, the percentage of all consumers who read most or all of their PFI's privacy policy is likely to be even less than 20%.*

[27] *"Edelman Trust Barometer 2021," Edelman, March 2021; "Fintech Apps and Data Privacy: New Insights from Consumer Research," The Clearing House, August 2018.*

[28] *Our findings did not indicate any major differences across these demographic groups. In some cases, the subsample of various demographic groups was too small to report on findings.*

Figure 16. Consumers strongly oppose opt-out standards and data sharing for marketing.

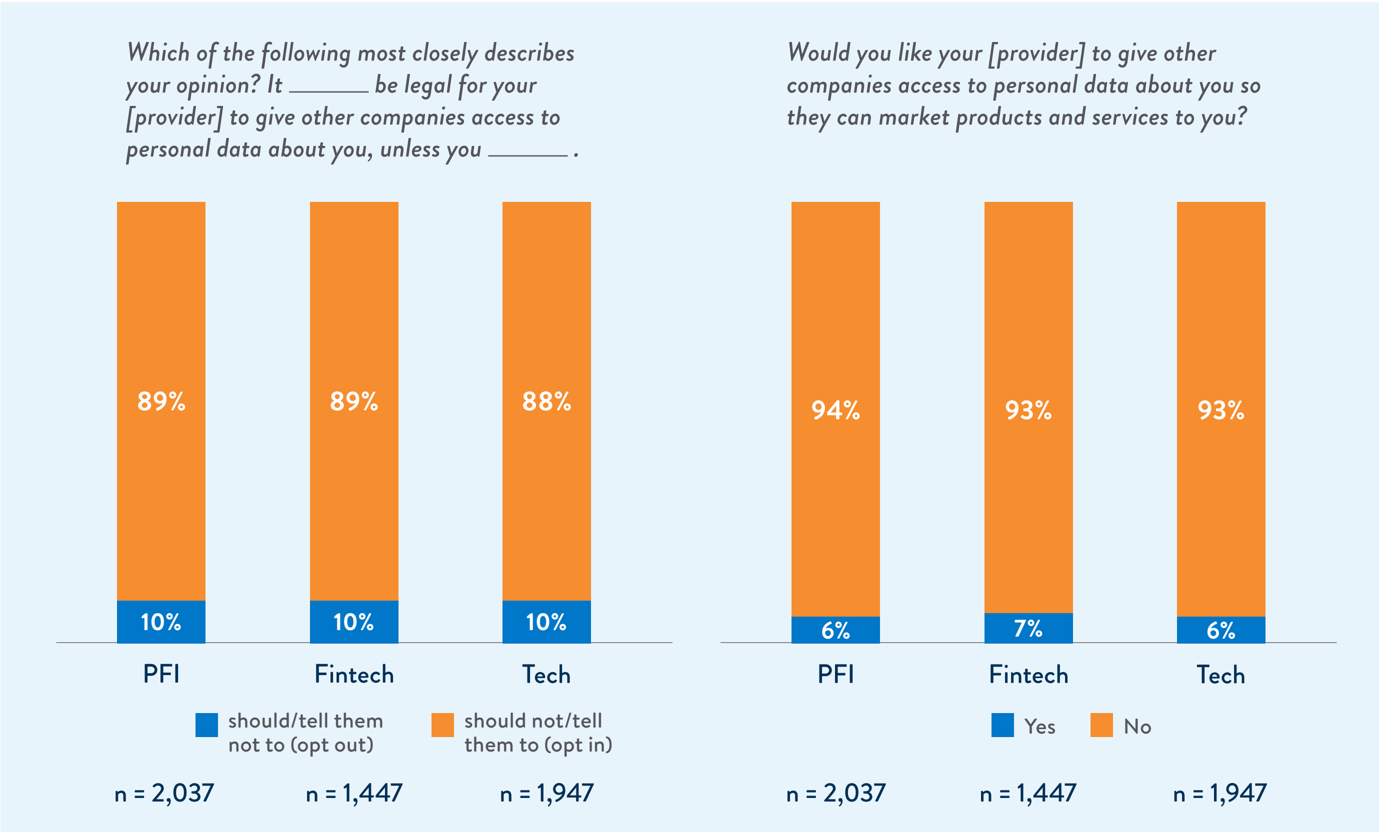
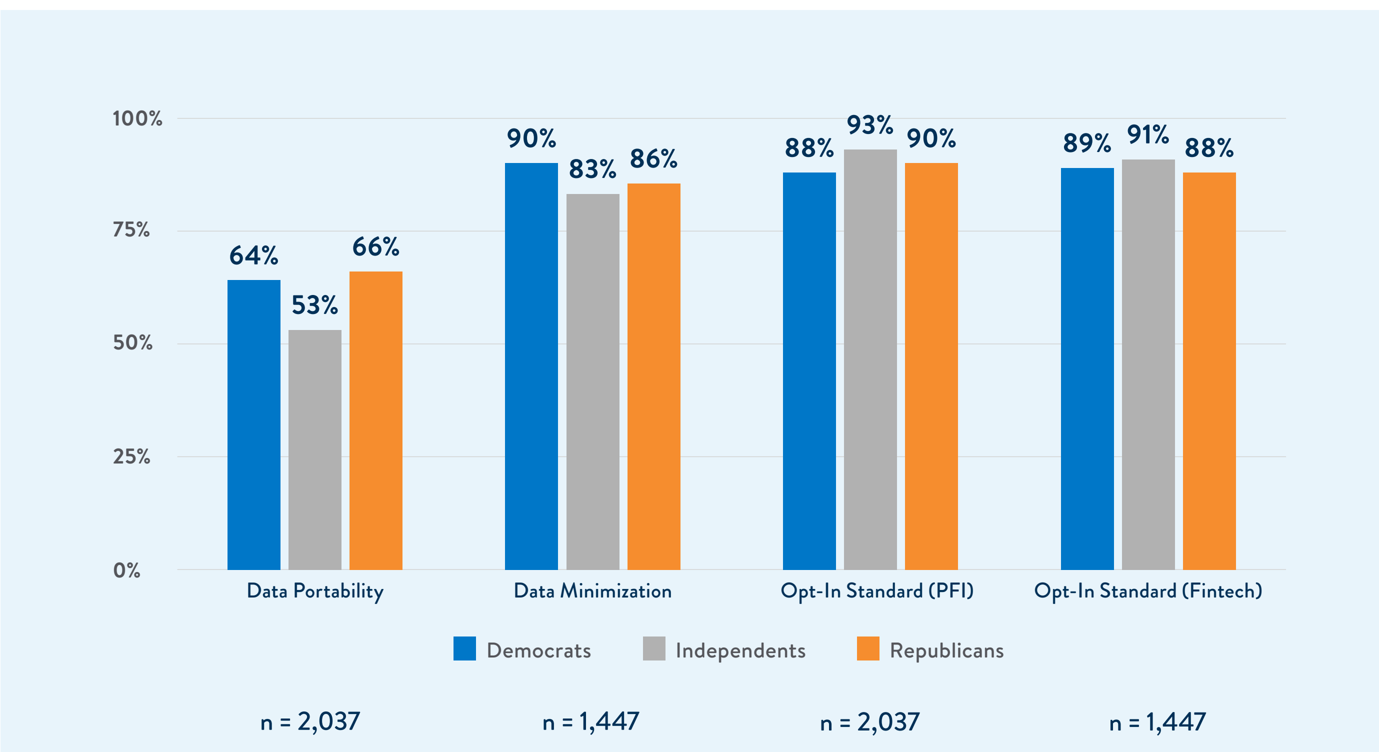


Figure 17. Consumers in favor of data portability, data minimization, and opt-in, by political affiliation.



Conclusion

The findings presented here describe the results of a nationally representative survey that was fielded to uncover consumer understanding and viewpoints on current practices in the financial data ecosystem.

We find that overwhelming majorities of consumers favor data minimization and opt-in standards and oppose data sharing for marketing purposes. We also find that a majority of consumers favor a right to data portability and believe their bank should be required to share data about them if they ask it to do so. These findings hold for every demographic group, including self-identified political party affiliation. The Financial Health Network hopes these results can serve as a guide to both industry stakeholders and policymakers who seek to maximize financial health, build trust, and ensure that both practice and policy serve consumer preferences.

Appendix

Methodology: Overall Weighted Demographics and Segments

We applied post-stratification weights to the full sample to make it nationally representative with respect to age, gender, census division, race/ethnicity, education, housing tenure, and household phone status. Instances in which the segments differ from the overall sample are marked with an asterisk (*) below. These asterisks indicate statistically significant differences from the corresponding overall column within a 95% confidence interval. The margin of error for the full sample is +/- 3.06 percentage points at the 95% confidence level.

		Overall (n = 2,037)	Technology Company Users (n = 1,947)	Fintech App Users (n = 1,447)	Online Lending (n = 1,292)	Online Lending + App Users (n = 1,565)
Gender	Male	48%	49%	51%	57%*	51%
	Female	52%	51%	49%	43%*	49%
Age	18-29	16%	17%	20%	20%	20%
	30-44	29%	30%	36%*	38%*	36%*
	45-59	24%	24%	22%	23%	22%
	60+	31%	28%	22%*	19%*	22%*
Race/Ethnicity	White	64%	63%	59%*	56%*	60%*
	Black	11%	11%	12%	14%*	12%
	Other	9%	9%	10%	11%	10%
	Hispanic	17%	18%	19%	19%	19%
Education	High School or Less	35%	33%	31%	33%	32%
	Some College	28%	28%	28%	29%	28%
	Bachelor's	19%	20%	22%	23%	22%
	Post Graduate	17%	18%	18%	15%	18%
Household Income	<$30,000	24%	23%	20%	19%	21%
	$30,000 to <$60,000	26%	26%	27%	26%	27%
	$60,000 to <$100,000	25%	25%	26%	30%	26%
	$100,000+	25%	26%	27%	25%	27%
Party ID	Democrat	49%	49%	52%	45%	51%
	Republican	35%	35%	34%	37%	35%
	Independent	17%	16%	15%	18%	15%

Methodology: AmeriSpeak® Panel

Funded and operated by **NORC at the University of Chicago**, AmeriSpeak® is a probability-based panel designed to be representative of the U.S. household population. Randomly selected U.S. households are sampled using area probability and address-based sampling, with a known, nonzero probability of selection from the NORC National Sample Frame. These sampled households are then contacted by U.S. mail, telephone, and field interviewers (face to face). The panel provides sample coverage of approximately 97% of the U.S. household population. Those excluded from the sample include people with P.O. Box-only addresses, some addresses not listed in the USPS Delivery Sequence File, and some newly constructed dwellings. While most AmeriSpeak households participate in surveys by web, noninternet households can participate in AmeriSpeak surveys by telephone. Households without conventional internet access but having web access via smartphones are allowed to participate in AmeriSpeak surveys by web. AmeriSpeak panelists participate in NORC studies or studies conducted by NORC on behalf of governmental agencies, academic researchers, media organizations, and commercial organizations. For more information, email AmeriSpeak-BD@norc.org or visit AmeriSpeak.norc.org.

NORC at the University of Chicago is an independent research institution that delivers reliable data and rigorous analysis to guide critical programmatic, business, and policy decisions. Since 1941, NORC has conducted groundbreaking studies, created and applied innovative methods and tools, and advanced principles of scientific integrity and collaboration. Today, government, corporate, and nonprofit clients around the world partner with NORC to transform increasingly complex information into useful knowledge. Please visit www.norc.org for more information.

FINANCIAL HEALTH
NETWORK

The Financial Health Network is the leading authority on financial health. We are a trusted resource for business leaders, policymakers, and innovators united in a mission to improve the financial health of their customers, employees, and communities. Through research, advisory services, measurement tools, and opportunities for cross-sector collaboration, we advance awareness, understanding, and proven best practices in support of improved financial health for all.

For more on the Financial Health Network,
go to **finhealthnetwork.org** and join the conversation online:

@FinHealthNet

Financial Health Network

Financial Health Network

Financial Health Network

EMERGE Blogs

Financial Health Network
135 S. LaSalle, Suite 2125, Chicago, IL 60603 | 312.881.5856