

AUGUST 2018



Executive Summary

Financial technology applications (fintech apps) have experienced a rapid rise in popularity in recent years. The appeal of these services is clear. From budgeting and payments to investing and lending, consumers find that managing their finances is often time-consuming and even confusing. Fintech apps provide solutions designed to be simple, fast and accessible via smartphones and tablets.

Despite the convenience they offer, fintech apps also pose risks. They require access to consumers' financial information, and the data collection process typically involves consumers sharing the log-in credentials for their bank accounts with the fintech apps or a data aggregator intermediary. After a third party has obtained a consumer's bank account log-in credentials, it can theoretically access any information on the consumer's bank account(s), perform any activity the consumer could and even share or sell the consumer's bank account information to others.

Recent data privacy events, such as the Facebook–Cambridge Analytica incident, have raised consumer awareness of data privacy and heightened concerns over collection and use of personal information. As consumers increasingly use fintech apps and provide access to their data, a crucial question is how aware those users are of how their data is accessed, collected, used, stored and shared. To better understand consumer perceptions and awareness of third-party personal and financial data collection, The Clearing House conducted a survey of more than 2,000 U.S. banking consumers and oversampled to reach 1,500 fintech users in Q1 2018.

What is a Data Aggregator?

What is a data aggregator? Data aggregators are companies that connect with financial institutions (e.g., banks, insurance companies or brokerages), collect customer data with the permission and on behalf of the customer, and provide that data to fintech apps. Some fintech apps perform data aggregation functions directly, without using an intermediary.



Key findings from the survey include:

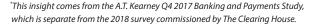
- One-third of U.S. banking consumers use at least one fintech app. Apps for personal financial management and budgeting/saving are the most popular services, followed by investment services and robo-advisors as well as lending services.
- Nearly nine in ten consumers (89%) said they are concerned about data privacy and data sharing—and more than two-thirds (67%) are very or extremely concerned.
- Consumers want to be able to control access to their information. A majority of respondents (56%) said they would like to determine which of their financial accounts and data types can be accessed by a third party.
- Most fintech app users believe they understand and can control how their data is accessed, collected, used and shared by third parties. But consumers' actual awareness of fintech data aggregation practices is often less. For example, after being told that many fintechs, as part of their terms and conditions, gain consent from consumers to use their data for purposes other than operating the app itself, nearly half of fintech users (47%) said they are now less likely to use these services.
- Banks are viewed as the most trusted provider of data security—and are expected to safeguard their customers' personal information. Banks led other providers by 13 percentage points when banking consumers were asked which organizations are best able to keep their personal information safe.*

The findings from the TCH survey underscore the need for collaborative action to ensure that the personal and financial information accessed by third parties is being handled securely and consumers' expectations for data security are being met. The financial services ecosystem is built on trust between consumers and companies; failure to live up to consumers' expectations and keep their information safe puts that trust at risk.

There is a need for a concerted effort by all stakeholders—including banks, fintechs, data aggregators, regulators, and consumers—to ensure data security.

TCH and its member banks are committed to:

- Expanding consumer awareness about how fintech apps access, collect, store, use and share users' personal and financial data;
- Developing principles, guidelines and technical standards to govern the collection, use and sharing of consumer data in the financial services ecosystem; and
- Promoting the use of technologies such as secure application programming interfaces (APIs), which offer a more secure and flexible alternative mechanism for third parties to access data.





KEY FINDING 1.

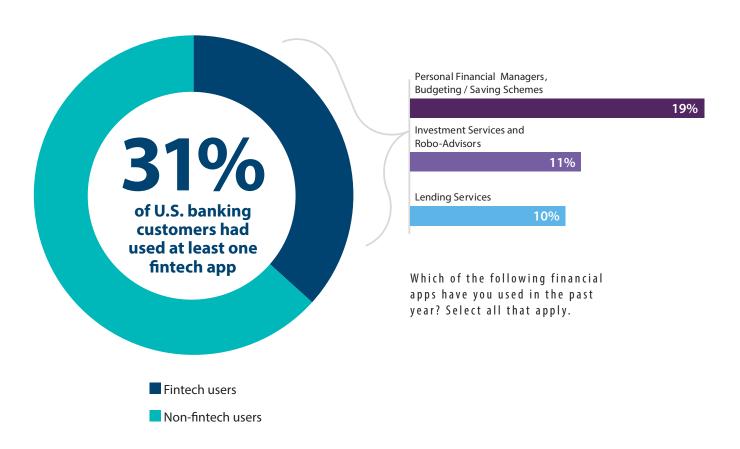
Nearly one-third of banking consumers use fintech apps, clustered around three application types.

Fintech apps have clearly gained a significant user base, with nearly one-third (31%) of U.S. banking customers indicating that they had used at least one fintech app in the past year. The most common fintech services were

personal financial management and budgeting/saving apps, followed by investment services and robo-advisors as well as lending services.

Distribution of fintech (non-bank financial application) users

% who use fintech apps among bank customers, by fintech app type



Most fintech users are concerned about data privacy and data sharing.

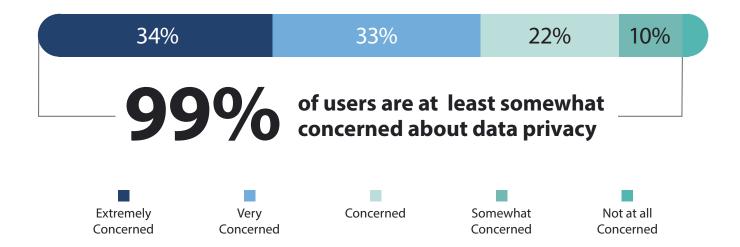
U.S. banking consumers who use fintech apps were asked how concerned they are about the privacy of the information that is shared when they use these apps either online or on a mobile device. Nearly nine in ten

(89%) said they are concerned—and more than twothirds (67%) are very or extremely concerned—about the privacy of their data

Level of concern regarding data privacy using fintech apps

% who selected each level of concern among a targeted population of fintech users

In general, how concerned are you about the privacy of the information that is shared when you use financial applications either online or on a mobile device?

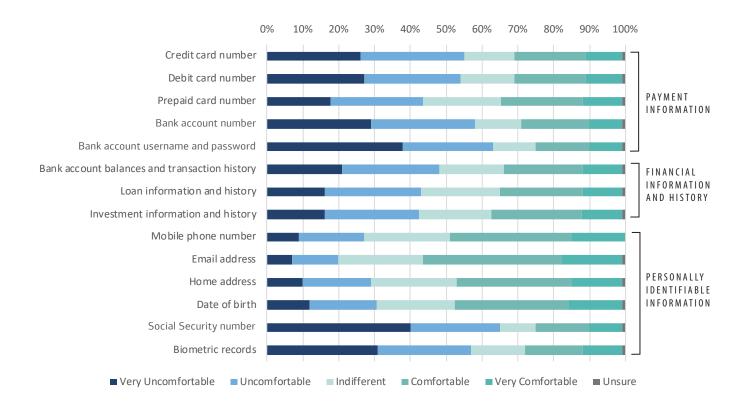


Fintech users' concerns about privacy extend to nearly all types of financial and personally identifiable information. For most payment information, as well as for financial information and history, roughly half of fintech users said that they are uncomfortable sharing this data with fintech apps. Consumers have the greatest concern about sharing their bank account username and password

and are least worried about fintech apps accessing their investment information and history. When it comes to more sensitive personally identifiable information, such as Social Security numbers and biometric records, around 60% of fintech users are not comfortable sharing their data with fintech apps.

Level of comfort sharing data with fintech apps

% who selected each data type among a targeted population of fintech users



How comfortable would you be with sharing the following personally identifiable information with financial applications you have used in the past year? To what extent are you comfortable with non-bank financial applications you have used in the past year accessing the following:



Consumers want to be able to control access to their information and have straightforward data privacy expectations.

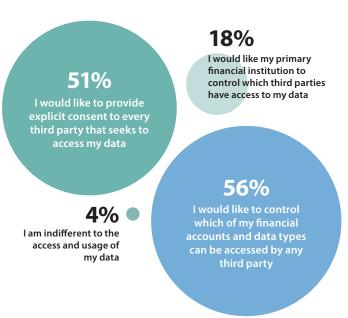
Privacy concerns are top of mind for consumers when they use fintech apps, and the survey findings make it clear that most fintech users want to be in control of who accesses their information. A majority of respondents (56%) said they would like to determine which financial accounts and data types can be accessed by a third party. Only 18% said they would like to leave these decisions to their primary financial institution.

When asked about their preferred mechanism for exercising control over third-party access to their data, half of consumers (50%) would like to have a permissions dashboard that they can access through their primary bank (i.e., the bank in which a consumer conducts their current transactions most frequently). A similar share (47%) would like to have a dashboard within the fintech apps they use.

Preferred third-party controls and access control mechanism(s)

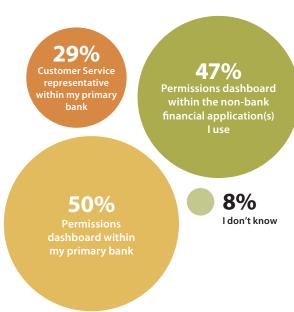
% who selected each data type among a targeted population of fintech users

How would you like to control third-party (e.g., financial applications, companies supporting the financial applications) access to, and use of, your data? Please select all that apply.



What would be your preferred mechanism to exercise control over third-party access, collection, use and sharing of your financial data?

Please select all that apply.



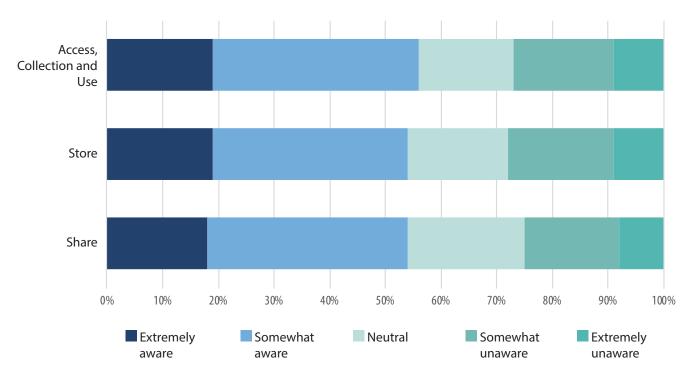
KEY FINDING 4.

Most fintech app users believe they are aware of, and can control, the ways in which their data is accessed, collected, used and shared by third parties.

More than half of consumers said that they are at least somewhat aware of how fintech apps interact with their personal and financial information.

Level of awareness of how fintech apps access, collect, use, store and share consumer personal and financial data

% who selected each level of awareness among a targeted population of fintech users

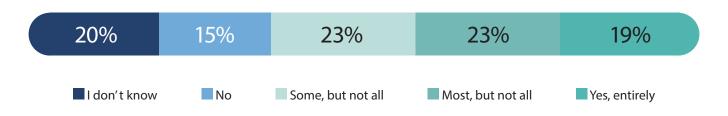


How aware are you of how financial applications access, collect, and use your personal and financial data? How aware are you of how financial applications store your personal and financial data? How aware are you of how financial applications, with your consent, share your data?

Fintech users also feel confident about their ability to control the flow of data to these apps. Nearly two-thirds (65%) of fintech users said that they can control how their data is accessed, collected, used and shared for at least some of the apps they use.

Consumer ability to control third-party access, collection, use and sharing of their data

% who selected each data type among a targeted population of fintech users



Do the financial applications you use today allow you to control how other third parties access, collect, use or share your data?

KEY FINDING 5.

Consumers' actual awareness of fintech data aggregation practices is less than their perceived awareness.

Despite data privacy being important to consumers who use fintech apps, the survey indicates that there is a significant gap between how people think these services interact with their data and how they work in reality. For

example, less than half of fintech users believe these apps can access their personally identifiable information or financial information and history—even though they often can (and do).

Consumer perceptions of data types accessible to fintech apps

% who selected each data type among a targeted population of fintech users



None of the above

To your knowledge, which types of data can be accessed by the financial applications you have used in the past year? Please select all that apply.

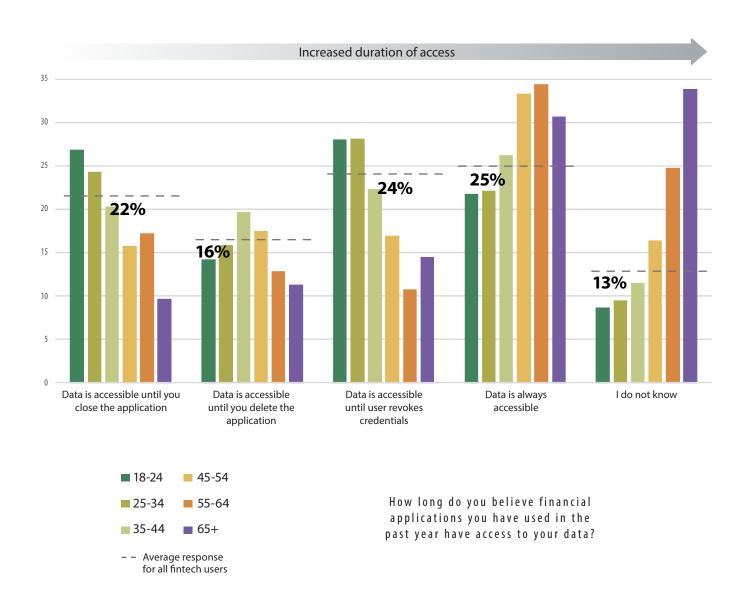
In addition to uncertainty about the scope of data access, consumers are also divided on how long fintech apps have access to their information. While the duration of data access may vary based on the individual fintech

app's terms and conditions, fintechs typically can access information so long as they have the user's valid log-in credentials.

Consumer perceptions of duration of fintech data access

% who selected each option among a targeted population of fintech users

However, roughly equal shares of respondents believe their data is accessible until they close the application (22%), until they revoke the log-in credentials for their bank account (24%) or that the information is always accessible (25%). There were notable differences between age groups on this question, too. Fintech users over the age of 45 were more likely to say they didn't know how long their data would be accessible. They were also more likely to say that their data is always accessible, while younger consumers disproportionately believe their data is not accessible after closing a fintech app.



Consumer perceptions of data usage by fintech apps

% who selected each option among a targeted population of fintech users



The discrepancy between fintech users' perceived awareness of how fintech apps access, collect and use their data and the actual practices becomes even more evident when consumers were asked about specific actions by fintechs. After being told that many fintechs, as part of their terms and conditions, gain consent from consumers to use their data for purposes other than

operating the app itself, nearly half of fintech users (47%) said that they are now less likely to use these services. Similarly, more than one in five fintech users (22%) said that they would not consent to a fintech app accessing their bank account credentials after hearing that these apps often store such credentials.

Consumer reaction to scope of fintech app data access, collection and use practices

% who selected each option among a targeted population of fintech users

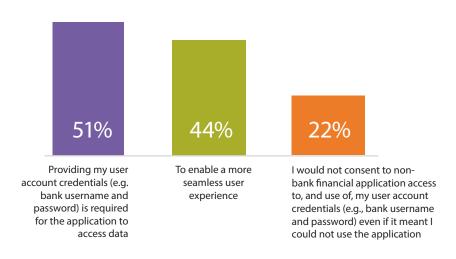


Many financial applications gain consent from their users to access, collect, and use personal and financial data for purposes other than your use of the application. Does this information change your attitude toward or willingness to use financial applications?

Consumer views on account credential storage by fintech apps

% who selected each option among a targeted population of fintech users

Financial applications often store user account credentials to access your account on your behalf and deliver you their products and services. For which of the following reasons would you allow applications to store your credentials? Please select all that apply.



KEY FINDING 6.

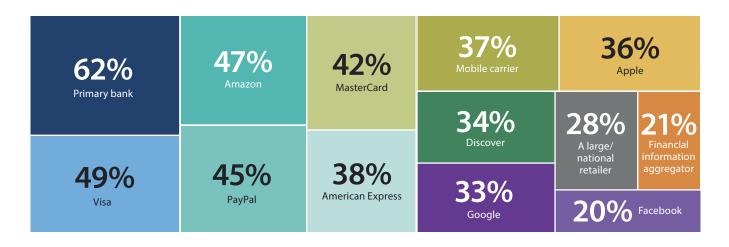
Banks are viewed as the most trusted provider of data security—and expected to safeguard the integrity of customers' personal information.

How do banks compare to fintech apps and other financial services providers in the realm of data privacy and data sharing? Previous research suggests that consumers place a high degree of trust in their primary bank. In a 2017 survey by A.T. Kearney, banks led other providers when consumers were asked which

organizations were best able to keep their personal information safe. More than three in five respondents (62%) said that their primary bank has that ability, while only 21% said the same about financial information aggregators.

Providers' ability to safeguard the security of customers' personal information

% who selected each provider among U.S. banking consumers*



Please rate the following firms on how well they safeguard the security of their customers' personal information.

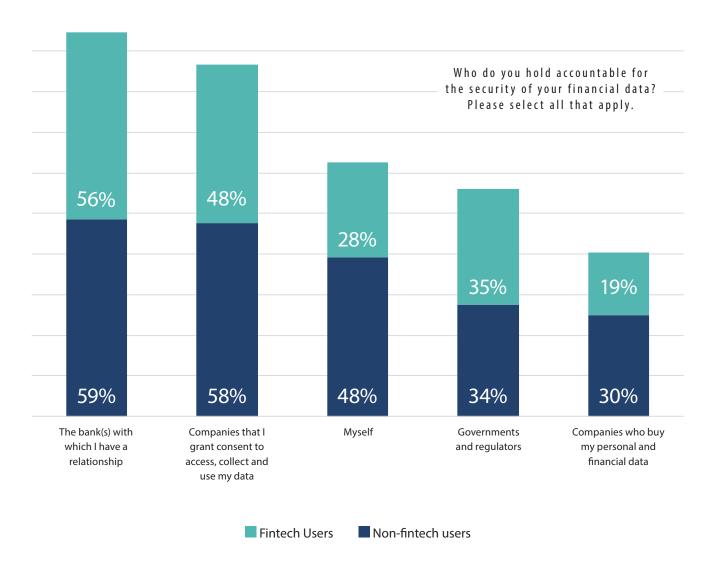


^{*}This insight comes from the A.T. Kearney Q4 2017 Banking and Payments Study, which is separate from the 2018 survey commissioned by The Clearing House.

Consumer views on accountability for financial data security

Important to note for banks is that they are not only seen as having the ability to keep their customers' personal and financial information safe; they are also expected to do so. In the TCH survey of more than 2,000 U.S. banking consumers, more than half of those who did use fintech

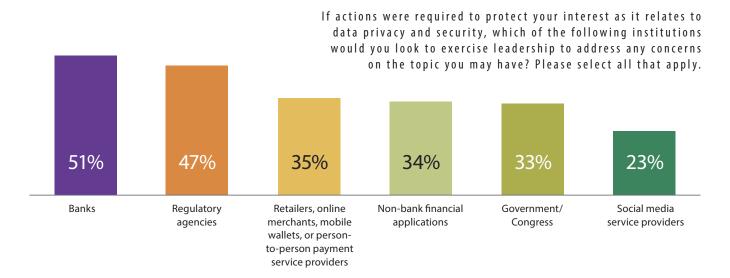
apps (56%) and those who did not (59%) said they hold the bank(s) with which these consumers have a relationship accountable for the security of their data.



Among fintech users, more than half (51%) said that they look to banks to protect their data privacy and security interests. By comparison, only about a third (34%) look to the fintech apps themselves. It's clear that consumers

have confidence in banks when it comes to keeping their data safe—and with that confidence come significant expectations.

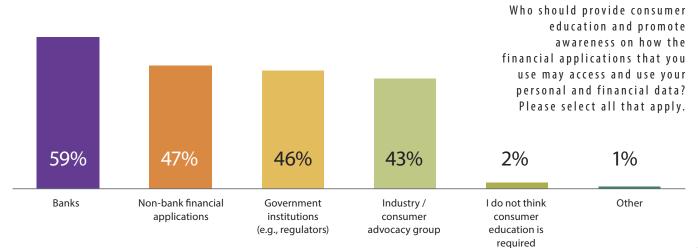
Consumer views on leadership regarding data privacy and security



One way in which banks can meet consumers' expectations is by providing educational materials about how fintech apps access, store, use and share consumer data. Roughly four in five fintech users (80%)

said that they are interested in learning more about these practices—and nearly three in five (59%) said that banks should provide the necessary information.

Entities that should provide consumer education and promote awareness on how fintech apps access and use consumer data



Recommendations

The findings from the TCH consumer survey underscore the need for industry action to ensure that the personal and financial information of fintech users is being handled securely and consumers' expectations for data security are being met. A collaborative crossindustry effort by all stakeholders—including banks, fintechs, data aggregators, regulators and consumers, among others—is required to achieve these goals. The following are initial (but by no means exhaustive) recommendations for creating an environment of stringent data privacy and security. TCH welcomes input from across the financial services industry and beyond to refine and expand these suggestions.

Further efforts to expand consumer awareness

The survey demonstrates a need for additional consumer education about how fintech apps access, collect, store, use and share users' personal and financial data. Fortunately, consumers realize that they face an information deficit, and many have a desire to learn. While consumers look primarily to banks to provide further education, significant numbers of fintech users said that fintech apps, government institutions and industry/consumer advocacy groups also have a role to play in raising public awareness. Industry stakeholders should come together and develop campaigns that provide consumers with a deeper understanding of data privacy and data sharing in the context of fintech apps.

Greater collaboration among industry stakeholders on principles, guidelines and technical standards

A collaborative approach should also be applied to the development of guardrails—both formal and informal—to govern the access, collection, use, storage and sharing of consumer data in the financial services ecosystem. Such guardrails should include principles and guidelines designed to improve the safety, security and transparency of sharing data with fintechs upon consumer request (e.g., through proposed consumer permission principles and controls). They should also include technical standards that enable safe and secure consumer data sharing.

Broader use of secure application programming interfaces (APIs)

While most fintech apps today rely on users providing their bank account log-in ID and password to access the data they need to provide their services, there is a secure and flexible alternative mechanism for third parties to access data. Application programming interfaces (APIs) allow banks to share information with data aggregators and other third parties in a way that is not dependent on the banks' customers offering up the log-in credentials for their bank accounts. APIs enable consumers to enjoy the advantages of fintech apps while providing them with greater control over the sharing of their data and maintaining the security of their account relationship. TCH strongly supports broader adoption of APIs within the financial services ecosystem.



Methodology

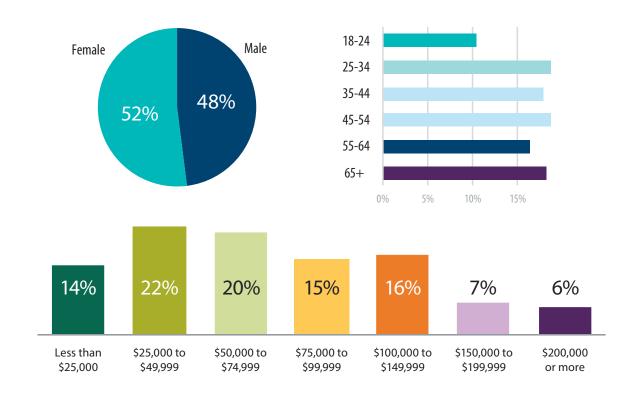
The consumer survey was conducted by A.T. Kearney on behalf of The Clearing House. The study was intended to address digital behaviors across banking customers, including user awareness of how third parties (i.e. non-bank fintech apps) access, collect, use, store and share their financial and non-financial data.

"Fintech apps" were defined as desktop or mobile financial applications that provide traditional banking services, including personal financial management services, budgeting/saving services, investment services, advisory services and/or lending services.

The survey was conducted in January 2018 with a nationally representative sample of more than 2,000 U.S. banking consumers who were at least 18 years of age. "Banking consumers" were defined as those who have a checking account, savings account, credit card, mortgage, personal loan or investment account with a financial services provider.

Overview of U.S. Banking Consumer Sample

(n=2,030)

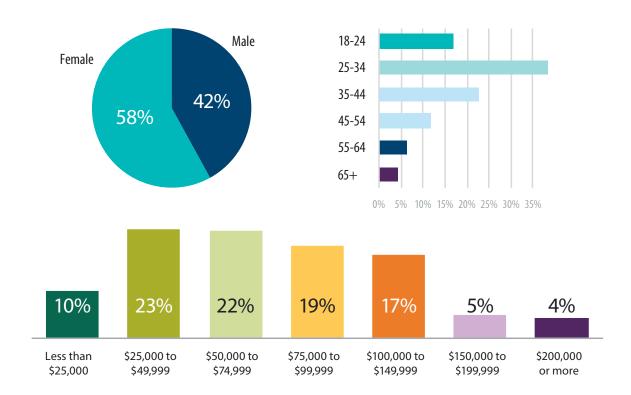


Of those respondents, 622 (30.6%) indicated they had used fintech apps in the past year. The survey over-sampled to target a population of fintech app users, which produced an aggregate fintech app

user population of ~1,500 U.S. banking consumers. The population of fintech users had a similar gender distribution as the broader, nationally-representative sample of U.S. banking consumers, but skewed younger.

Overview of U.S. Fintech User Sample

(n=1,504)



Findings were captured by holding an online panel and asking questions regarding:

- Banking relationships and primary bank incidence
- Primary bank relationships (e.g., banks with which a consumer conducts their current transactions most frequently)
- Banking channel usage
- Digital purchase incidence and behavior
- Data privacy and sharing preferences
- Consumer control of third-party access
- Consumer education channel preferences

About The Clearing House

Since its founding in 1853, The Clearing House has delivered safe and reliable payments systems, facilitated bank-led payments innovation, and provided thought leadership on strategic payments issues. The Clearing House continues to leverage its unique capabilities to support bank-led innovation, including launching RTP®, a real-time payment system that modernizes core payments capabilities for all U.S. financial institutions. The Clearing House is the only private-sector ACH and wire operator in the United States, clearing and settling nearly \$2 trillion in U.S. dollar payments each day, representing half of

all commercial ACH and wire volume. As the country's oldest banking trade association, The Clearing House also provides informed advocacy and thought leadership on critical payments-related issues facing financial institutions today. The Clearing House is owned by 25 financial institutions and supports hundreds of banks and credit unions through its core systems and related services. Learn more at www.theclearinghouse.org.

About A.T. Kearney

A.T. Kearney is a leading global management consulting firm with offices in more than 40 countries. Since 1926, we have been trusted advisors to the world's foremost organizations. A.T. Kearney is a partner-owned firm,

committed to helping clients achieve immediate impact and growing advantage on their most mission-critical issues. For more information, visit www.atkearney.com.

