February 4, 2021

VIA ELECTRONIC MAIL (2020-ANPR-1033@cfpb.gov)
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

Re: Docket No. CFPB-2020-0034 / RIN 3170-AA78
ANPR – Consumer Access to Financial Records

Ladies and Gentlemen:

The Clearing House Association (TCH)[1] appreciates this opportunity to respond to the Bureau of Consumer Financial Protection's Advanced Notice of Proposed Rulemaking (ANPR) on "Consumer Access to Financial Records"[2] through which the Bureau is soliciting comments and information to assist the Bureau in developing regulations to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[3] TCH notes that the Bureau has engaged in considerable prior work in this area, including a previous Request for Information on *Consumer Access to Financial Records* in November of 2016,[4] the release of the Bureau's *Principles for Consumer Authorized Financial Data Sharing and Aggregation* (Principles) in October of 2017[5] and, more recently, arranging a symposium on *Consumer Access to Financial Records* in February of 2020.[6] TCH appreciates the thoughtfulness with which the Bureau has approached its work in this complex area.

TCH and its member banks are fully supportive of and, as more fully detailed in this letter, have engaged in significant work with other industry stakeholders to facilitate the ability of consumers, upon request, to safely and securely obtain information about their ownership or use of a financial product or service from their product or service provider. As the Bureau notes in the ANPR, "various market participants have helped authorized data access become more secure, effective and subject to consumer control."[7] It will be important that whatever further action the Bureau takes in this area

[1] The Clearing House Association L.L.C. is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound, and competitive banking system.
[2] Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (Nov. 6, 2020).
[3] *See* 12 U.S.C. § 5533.
[4] Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83,806 (Nov. 22, 2016).
[5] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf (accessed Jan. 3, 2021)).
[6] *See* Consumer Financial Protection Bureau, "Bureau Symposium: Consumer Access to Financial Records, a summary of the proceedings" (July 24, 2020) (summarizing the Bureau's symposium) (available at: https://www.consumerfinance.gov/data-research/research-reports/bureau-symposium-consumer-access-financial-records-summary-proceedings/ (accessed Jan. 3, 2021)).
[7] 85 Fed. Reg. at 71,003.

enhance, rather than inhibit, the substantial progress that has been made. Further, we note that any rulemaking in this area is likely to be complex, time-consuming, and require the substantial commitment of both short-term and long-term resources by the Bureau in order to be successful. It will also need to envision the state of a rapidly developing market several years into the future – the approximate time it would take to promulgate a rule and have the rule become effective. Such an undertaking may pose substantial risks to further industry progress if the industry were required to await key decisions from the Bureau on the path forward. For all those reasons, further developing guidance in a manner consistent with the Principles may be preferable. At the same time, TCH acknowledges that the Bureau may nonetheless determine to proceed with a rulemaking, and TCH has set forth in this letter the issues that TCH believes such a rulemaking should address if the Bureau chooses to take this path. In either case, however, it is imperative that further action taken by the Bureau align with the Principles, which have provided the basis for so much industry progress to date. Early assurances of such alignment will be helpful in allowing the industry to continue progress while the Bureau engages in further work and deliberation. It is also imperative that there be interagency coordination to ensure that the federal financial services regulators are coordinated on their approach and speak with one voice.

TCH notes that the FI data holders[8] that comprise TCH's membership often play a dual role in the data sharing ecosystem in that they are often significant data users[9] as well. It should be noted that the recommendations TCH is making for areas that should be addressed in the event the Bureau proceeds with a rulemaking would apply to TCH's members in their roles as both FI data holders and data users.

Fundamentally, TCH agrees with the Bureau's assessment that "some emerging market practices may not reflect the access rights described in section 1033."[10] TCH would add that some market practices do not reflect the Bureau's fundamental vision for data sharing as outlined in the Bureau's Principles, which contemplate a consumer-centric approach that emphasizes consumer control and protection. TCH's own efforts to further the development of safer, more secure and transparent data sharing practices have been guided by the Principles, with which TCH and its members are fully aligned. TCH believes that many of the answers to questions posed by the Bureau in the ANPR can be deduced from an analysis of the Principles and an examination of existing market practices and initiatives, and whether those market practices and initiatives are likely to be able to achieve, absent further action by the Bureau, the desired state that the Principles outline. Based on that analysis, which is more fully set forth herein, TCH makes the following recommendations:

1. Further guidance consistent with the Principles may be preferable to a rulemaking given the complexity, time and resource commitment required by the Bureau to engage in a successful rulemaking and the potential for delay and uncertainty to freeze progress that the market has been making;

[8] TCH has incorporated the Bureau's definitions as set forth in the ANPR in this letter. The Bureau has defined "data holder" as "a covered person with control or possession of consumer financial data." 85 Fed. Reg. 71,003, at 71,004. Other Bureau-defined terms used throughout this letter include "authorized data access," "authorized entities," "data aggregator," and "data user."

[9] The Bureau has defined "data users" as "a third party that uses consumer-authorized data access to provide either (a) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer." *Id.*

[10] *Id.*

2. TCH believes that the Bureau should continue to rely on private sector market-led efforts for technical standard setting of the kind engaged in by FDX and believes it would be a mistake for the Bureau to attempt to define technical standards. There are a number of actions that the Bureau could nonetheless take that would be consistent with the Bureau's charge in Section 1033 to "promote" the development and use of standardized formats for information. These include:
    a. Finding ways to explicitly endorse or reference technical standards and certification organizations like FDX and the work that they are doing,
    b. Providing greater regulatory clarity on the issues discussed below and thereby allowing the industry to then work together to develop or further enhance existing standards to implement the CFPB's vision, and
    c. Working with other regulators to ensure that the Federal financial regulators are speaking with one voice on issues affecting the data aggregation market.
3. If the Bureau is determined to proceed with a rulemaking, the rulemaking must be holistic in its approach and, at a minimum, address the following issues that are discussed more fully below:
    a. Credential sharing and credential storage as well as screen scraping pose significant risks to consumers, including risks related to data breaches and fraudulent and unauthorized transfers as well as identity theft and other data privacy issues, and should be abolished as a fundamental part of any rulemaking. Such action could take the form of the Bureau articulating a rule that prohibits a data aggregator or data user from obtaining consumer data using a consumer's online banking credential and screen scraping where a data holder has provided the data aggregator or data user with the option of enabling safer, more secure methods, such as API access under fair and reasonable terms. The Bureau may also wish to consider a rule that sunsets credential-based data sharing, storage and screen scraping upon a schedule that would be phased in over time by institutional size.
    b. The Bureau in any rulemaking should clarify that data access is limited to circumstances in which a data user will provide services to the consumer that is providing the data, reasonably requires the data to provide those services and does so in a way that is transparent and consistent with consumer expectations. If data is sold to third parties for use in research or analytics unrelated to the underlying service, that information should be clearly and conspicuously disclosed to consumers and subject to their consent.
    c. The Bureau in any rulemaking should develop disclosure requirements for all parties, including model disclosures that create a safe harbor for various stakeholders. Requirements must recognize that FI data holders will have limited visibility into data usage and downstream parties. Accordingly, data holders should generally be limited to disclosing to whom the data is initially being provided, the fact that the provision of data was authorized, and identification of the appropriate mechanism through which the consumer may halt the ongoing provision of data. Data aggregators and data users should be required to disclose to consumers the identity of each data user to which the consumer's data is being provided and each data user with whom information is shared should be required to obtain separate and distinct authorization from the consumer for the use of the consumer's data. Disclosure should include what data is being accessed, how frequently it is being accessed, for what

purpose, and for how long it is being stored. Disclosures must be sufficiently clear and easily understood by consumers to ensure that authorization is knowingly given, and mandatory periodic affirmative reauthorization should be required no less frequently than annually. Disclosures should also clearly spell out the consumer's right to revoke authorization and should include the right to be forgotten. The Bureau should impose a heightened "clear and conspicuous" standard for consent relating to the sale of consumer data unrelated to the direct provision of any service to the consumer.

d. The Bureau in any rulemaking should clarify that the concept of a "trusted third party" recipient of data requires trust not only by the consumer, but also requires that the data aggregators and data users will have satisfactorily met the FI data holder's own reasonable risk management criteria in order to qualify to receive the data. Given the risks that data aggregators and data users introduce into the ecosystem, such requirements should include not only appropriate information security controls, but also insurance and financial requirements that are commensurate to the risks being introduced.
e. Regardless of the requirements of any technical standard being applied, the Bureau in any rulemaking should clarify that the standard must be subservient to an overall data minimization principle – that a data aggregator or data user should still only obtain and use data strictly as needed for the service currently being provided, and, further, that the consumer should be fully in control of what categories of data are being provided, to whom, for how long, and for what purpose, regardless of use case.
f. The Bureau in any rulemaking should clarify the nature and extent to which confidential information may be protected from disclosure and should specifically extend the protection for confidential information to commercially sensitive trade secrets that are not otherwise disclosed to consumers. Similar to the prohibitions on reverse engineering that are found in most data aggregator and data user agreements, the protection for confidential information should include a prohibition on the reverse engineering of proprietary algorithms and other processes that are not otherwise disclosed to consumers.
g. The Bureau in any rulemaking should clarify that FI data holders, who are mere conduits for information being pulled by data aggregators and data users acting as agents for FI data holder customers, are not "furnishers" for purposes of the Fair Credit Reporting Act.
h. The Bureau in any rulemaking should recognize that the use of data to facilitate the movement of money carries heightened risks for consumers and for FI data holders relating to unauthorized payments and fraud and should affirm the legitimacy of FI data holders imposing reasonable, heightened requirements for the disclosure of information that can be used to initiate payments, including the imposition of enhanced security measures such as tokenization, enhanced due diligence, and enhanced information security controls.
i. In order to ensure that sensitive consumer financial information is appropriately protected throughout the data lifecycle, the Bureau in any rulemaking should subject data aggregators that are the recipients of such data to functionally similar requirements to those imposed on FI data holders when handling the same information. Data aggregators should also be subject to supervision and

enforcement to ensure compliance and should be responsible for passing on and enforcing security requirements to data users.

j. The Bureau in any rulemaking should recognize and affirm the legitimate role that FI data holders play in protecting their customers and the financial system and should affirm an FI data holder's ability to control access, affirm authentication and impose reasonable time, place and manner restrictions in circumstances that are consistent with protecting the consumer and the safety and soundness of the financial system. This should include any circumstances in which the FI has a good faith belief that access may be fraudulent, may present security risks to the consumer, the FI or the financial system generally, may relate to misuse of the consumer's data or may relate to data beyond that which is reasonably related to the product or service being provided to the consumer or as reasonably needed to protect the security, efficiency and operational integrity of the FI data holder's own systems

k. The Bureau in any rulemaking should make allowance for FIs to obtain data usage information from data aggregators and data users so that they may voluntarily provide it to consumers if the FI has the ability to provide the consumer with a one-stop, aggregated view of the consumer's data usage. Such an aggregated view is clearly beneficial to consumers and should be encouraged by the Bureau where possible in order to help the consumer be an active participant in stewarding their data.

l. The Bureau in any rulemaking should interpret the need for data accuracy consistent with data holders making available information that is subject to an FI data holder's standard posting times and other procedures that the FI has adopted for data handling in the ordinary course of its business, which is the standard imposed by Section 1033. The Bureau should recognize that FI data holders will have limited understanding and control over downstream uses of data and therefore cannot be guarantors that data accessed will be accurate and current for all purposes and in all circumstances.

m. FI data holders are already subject to robust regulations and requirements relating to addressing claims of unauthorized access and other consumer disputes and have substantial resources and processes in place to address such issues. Data aggregators and many data users, however, do not. Accordingly, any rulemaking engaged in by the Bureau should adopt a dispute resolution infrastructure outlining minimum standards for data aggregators and data users commensurate with those already imposed on FI data holders.

n. Any rulemaking engaged in by the Bureau should prohibit data aggregators and data users from disclaiming liability to either the consumer or the data holder for acts or omissions relating to data while it is in their custody or control, which is today a common practice. Liability should follow the data and all parties should be fully accountable for its care.

o. In order to ensure that consumers are protected and that there is an appropriate trust environment for the sharing of data, any rulemaking by the CFPB should include an assertion of the Bureau's authority under Section 1024(a)(1)(B) or Section 1024(a)(1)(c) of the Dodd Frank Act and allow for the appropriate supervision and examination of data aggregators with appropriate requirements for data aggregator due diligence and oversight of data users with whom consumer information is shared. FI data holders are already subject to

robust supervision and enforcement. Supervision and enforcement of data aggregators is a fundamental component that would be needed to ensure meaningful compliance with any rules developed by the Bureau.

p. The Bureau should study and evaluate the requirements set forth in Regulation E, which predate the substantial changes that have taken place in the marketplace and that have been facilitated by data aggregation and other activities. Data aggregation activities are increasingly being leveraged to enable payment initiation. Those services frequently exist outside of the control of FI data holders and yet liability for unauthorized transfers and the costs of recredentialing continue to rest with them. Incentives may need realignment to ensure that parties are properly incented to appropriately protect the data that is in their care.

I. *Principles for Consumer Authorized Financial Data Sharing and Aggregation*

The Bureau's most important work to date on issues relating to Section 1033 has been the development and release of the Principles in October of 2017. The Principles, which took into consideration feedback provided by a wide range of stakeholders in response to the Bureau's prior RFI, set forth the Bureau's vision for how consumers should be protected when they authorize third party companies to access their financial data to provide certain financial products and services.[11] The Principles were "intended to help foster the development of innovative financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives."[12] The Principles are fully supported by TCH and its member banks, have guided the work of TCH and other industry stakeholders as we have sought to implement the Bureau's vision, and remain highly relevant today. Since their release in 2017, much has been accomplished by the industry as it has worked towards making the Bureau's vision a reality, driven by a shared desire to protect consumers and the safety and security of the financial services ecosystem as the market for services using consumer-authorized financial data continues to develop. While the Principles have been a useful tool in guiding the industry's work and much has been accomplished in reliance on them, there are areas, as discussed more fully below, where further action by the Bureau would be useful. In order to continue the industry's momentum, however, it is imperative that any further action taken by the Bureau be consistent with the Bureau's prior positions articulated in the Principles and be coordinated with other federal financial services regulators to ensure a consistent approach to issues relating to consumer-permissioned data access. Such a consistent approach is essential to avoid bifurcating the market, which could greatly inhibit the scalability of industry standards, utilities, and other solutions.

[11] Consumer Financial Protection Bureau, "CFPB Outlines Principles For Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017) (available at: https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/ (accessed Jan. 3, 2021)).

[12] *Id.*

II. Industry Initiatives

a. TCH Connected Banking Initiative

TCH's Connected Banking initiative seeks to enable "innovation and customer control through a more secure exchange of financial data."[13] The initiative recognizes the need to move beyond a system of credential-based data access and screen scraping and to a safer, more secure, more transparent and consumer-centric API environment.

The terms "credential-based data access" and "screen scraping" may sound innocuous, but they are not. Credential-based data access involves consumers sharing their internet banking platform login credentials (user ID and password) with a third party. These are the same login credentials that consumers use to authenticate into their internet banking platform in order to move money and initiate other financial transactions and services. When a consumer shares their login credentials, FI data holders may not be able to distinguish whether the login credentials are being used by the consumer, an authorized third party or a fraudster. Indeed, it is interesting to note that some data aggregator and data user agreements reviewed by TCH *prohibit* the data aggregator's or data user's customers from sharing the data aggregator or data user's internet platform login credentials (provided by the data aggregator or data user) with any third parties, such practice apparently being viewed by those data aggregators and data users as a significant risk to their own data security and integrity. [14]

Similarly, the process of screen scraping also carries certain risks. Screen scraping refers to the practice by which a data aggregator or data user employs automated processes to "scrape" data from the FI data holder website. In most circumstances, such data includes far more data than is actually needed to power the product or service being provided, including personally identifiable information or other details that the consumer may not have authorized if the process were more transparent to and capable of being controlled by the consumer. In addition, screen scraping is more prone to inaccuracies and has the potential of creating operational challenges for FI data holders.

APIs offer significant advantages to credential-based data access and screen scraping. As the CFPB Taskforce Report notes:

> An API is a structured data feed that connects the account holder, such as the consumer's bank, to the data aggregator [Note omitted.] Because an API requires an agreement between the account holder and the data aggregator, parties to an API have the opportunity to agree on terms regarding the scope of data that the account holder will provide to the data aggregator, how often the account holder will provide or

---

[13] Detailed information regarding TCH's Connected Banking initiative is available at: https://www.theclearinghouse.org/connected-banking (accessed Jan. 3, 2021).

[14] *See, for example,* Plaid, "End User Privacy Policy," at "Registration" (Dec. 30, 2019) (providing that users "may never share [their] Account information, including [their] Plaid Dashboard password, as well as [their] API authentication credentials, including [their] Client identification Number ('Client ID') and secret, with a third party of allow any other application or service to act as you"); *and* Robinhood Financial LLC & Robinhood Securities, LLC, "Customer Agreement," at "K.Electronic Access" (Dec. 30, 2020) (prohibiting Robinhood users from sharing their usernames and passwords with any third parties).

update that information, limits on the data aggregator's use or resale of data, and other terms, such as the parties' respective liabilities to each other and the consumer.

APIs do not require consumers to provider their security credentials to the data aggregator; instead, the consumer can authenticate the aggregator with the financial institution, and the institution will provide an access token to the aggregator. As a result, an API may limit a data aggregator's access to certain account information or account services, such as making electronic fund transfers.[15]

To facilitate the shift from credential-based access and screen scraping to APIs, TCH is actively engaged in the development of new technology standards, infrastructure, innovative solutions to address risk management requirements and legal agreements, and in ongoing industry collaboration.[16] The initiative is guided by the goal of acting "in the best interest of consumers [to] enhance safety and foster efficiency in financial services."[17]

TCH's Connected Banking initiative has resulted in a number of important deliverables:

- Model Agreement: In order to enhance consumer control over the data they share with data aggregators and data users and to provide for a safer and more secure method to facilitate such sharing, the Connected Banking initiative has focused on accelerating the ability of data holders, data aggregators[18] and data users to establish safe and secure direct connections through application programming interfaces (APIs). Recognizing that legal agreements between data holders and authorized entities[19] can take considerable time and resources to develop, TCH, in collaboration with its member banks and in consultation with data aggregators and data users, developed a Model Agreement that can be used as a reference to facilitate the development of API-related data sharing agreements. The Model Agreement was based on a number of already existing bilateral agreements in the market and was specifically developed to be consistent with the Bureau's Principles and focus on consumer control and transparency, safety and security

[15] CFPB Taskforce Report, Vol 1, pp. 489-490.
[16] *Id.* The work being done by TCH is specifically acknowledged in the CFPB Taskforce Report. *See, CFPB Taskforce Report*, Vol 1, p. 495, note 139.
[17] *Id.*
[18] The Bureau has defined "data aggregator" as "an entity that supports data users and/or data holders in enabling authorized data access." *Id.* According to the Bureau's Taskforce on Federal Consumer Financial Law ("Taskforce"), which released a two-volume report on January 5th ("CFPB Taskforce Report") containing recommendations on how to improve consumer protections in the financial marketplace, "there may be at least 120 or as few as a handful of firms that engage in this activity." The CFPB Taskforce Report notes a Vermont law that requires parties that buy or sell third-party data to register with the secretary of state and that as of March 2019, 121 firms had registered. The CFPB Taskforce Report further notes that some of these entities – such as the National Student Clearinghouse and the nationwide consumer reporting agencies – are not typically thought of as data aggregators in the consumer finance market, even though they gather and provide consumer data. "Focusing more narrowly on financial data aggregators," the CFPB Taskforce Report posits that "there are as few as six significant firms in the market." CFPB Taskforce Report, Vol 1, pp. 494-495.
[19] The Bureau has defined "authorized entities" as "entities or persons with authorized data access to particular consumer financial data." *Id.*

of the data, and appropriate accountability for any risks introduced into the system.[20] Bilateral agreements play a vital role in today's data sharing market. In the absence of a further legal framework being developed through regulatory action or otherwise, bilateral agreements are the only way that FI data holders can allocate liability, ensure transparency and consumer control, and address many other fundamental issues.[21]

- API Technical & Security Standards: TCH and many of its member banks are founding members of the Financial Data Exchange (FDX), which was created to provide an organization through which cross-industry participants could develop, maintain, and facilitate the adoption of common API standards for sharing consumer financial data.[22] More detailed information on the work of FDX is provided below.
- Uniform Assessment Instrument: Meeting regulatory expectations for due diligence on parties with whom an FI data holder is sharing data (either through an API or otherwise) can be significantly burdensome in terms of time and resources committed for both the FI performing the due diligence and the data aggregator or data user on whom due diligence is being performed, with each FI historically performing one-off due diligence inquiries.[23] In order to create efficiencies and encourage the development of API relationships, TCH developed a uniform assessment instrument being implemented in the market today that streamlines due diligence, allowing due diligence information to be collected once by assessment vendors and then shared by assessment vendors with multiple FIs through their secure portal thereby alleviating largely redundant processes across the financial ecosystem.
- Central Utility Option: TCH and a number of its member banks played a pivotal role in the spinout of Akoya L.L.C. ("Akoya") from Fidelity Investments, Inc. and the positioning of Akoya to provide an option that solves for connectivity issues in an API-reliant ecosystem. The role Akoya is anticipated to play in the market is discussed in more detail below.
- Consumer Research: TCH's Connected Banking initiative has been further guided by in-depth consumer research detailing consumer preferences and awareness regarding the data practices of the financial applications they use. Key findings include:

---

[20] More information on the Model Agreement is available at: https://www.theclearinghouse.org/connected-banking/model-agreement (accessed Jan. 7, 2021).

[21] While bilateral agreements may be needed for some time in the future, it is anticipated that small banks will ultimately be able to leverage bilateral agreements between their third-party service providers and data aggregators and data users. There is also the potential for entities that play a central utility role, like Akoya, to develop common rule sets or agreements that may ultimately take the place of some or all of the content that is covered in bilateral agreements today.

[22] Additional information on TCH's support for FDX is contained in: The Clearing House, "The Clearing House Supports Financial Data Exchange Work on API Technical Standards" (Oct. 18, 2018) (available at: https://www.theclearinghouse.org/payment-systems/articles/2018/10/data-privacy-10-18-2018 (accessed Jan. 7, 2021)).

[23] *See*, *for example*, OCC, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2013-29 (Oct. 30, 2013) (available at: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html (accessed Jan. 7, 2021)), *and* OCC, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulleting 2013-29," OCC Bulletin 2020-10 (March 5, 2020) (available at: https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html (accessed Jan. 7, 2020)) (FAQ #4, in particular, relates to the application of OCC guidance to data aggregation relationships).

- Consumers want more education and control over access to their information;
- While consumers tend to feel secure about using financial applications, most are unclear about the terms and conditions of the services they have signed up for;
- When they learn more about the actual practices of the data users that provide them with the financial applications they use, their trust in data privacy and security is eroded; and
- Most consumers are not aware of what personal and financial information financial applications have access to, for how long, and what actions the application service provider can take with their information.[24]

b. FDX

FDX is an international, nonprofit organization operating in the US and Canada that is dedicated to unifying the financial industry around the FDX Application Programming Interface (FDX API), which is a common, interoperable, royalty-free standard for the secure access of permissioned consumer and business financial data. FDX has broad stakeholder representation and is currently comprised of 167 data holders (i.e., financial institutions), data users (i.e., third-party financial technology companies or fintechs and financial institutions[25]), data access platforms (i.e., data aggregators and other ecosystem utilities), consumer groups, financial industry groups and other permissioned parties in the user-permissioned financial data ecosystem.

FDX exists chiefly to promote, enhance and seek broad adoption of the FDX API technical standard, which allows for consumers within the financial data ecosystem to be securely authenticated without the sharing or storing of their login credentials with third parties. Broad adoption of the FDX API standard helps to transition the industry away from screen scraping (the retrieval of financial account information with a user's provided login credentials) and enhances the security and reliability of the flow of user-permissioned data between data holders, data aggregators, and data users. Moving the industry to API based access is important for a number of reasons. Most importantly, the use of credential-based access and screen scraping requires the sharing of sensitive consumer login credentials and provides limited consumer control over the amount of data consumers share with data aggregators and data users. Credential based access and screen scraping are also inefficient and can place stress on financial institutions due to the sheer number of automated logins. Consumers and financial institutions also bear significant risks associated with potential data breaches at data aggregators and data users and the potential for losses attendant to login credentials and other sensitive consumer information coming into the possession of fraudsters.

The FDX API technical standard seeks to replace the practice of credential-based data access and screen scraping with tokenized access in concert with API-based data collection, which allows a consumer to be securely authenticated at their own financial institution and permission only the data

[24] *See* The Clearing House, "Consumer Survey: Financial Apps and Data Privacy," p. 3 (Nov. 2019) (noting that "[m]ost financial app users are not aware of the personal and financial data the apps have access to") (available at: https://www.theclearinghouse.org/-/media/new/tch/documents/data-privacy/2019-tch-consumersurveyreport.pdf (accessed Jan. 7, 2021)).

[25] Many FIs are both data holders and data users.

that the consumer would like to share. APIs provide the ability for the consumer to choose the type of data that is shared, with whom, for how long, and for what purpose. A standardized API along with other standards that have either been or are being created by FDX (such as authentication, authorization, certification, user experience and consent guidelines) create efficiencies in the ecosystem that help speed the adoption of API based data sharing. Without the FDX standards, the ecosystem would remain fragmented – using incompatible APIs, process and definitions. As a result of the development of the FDX API, over 12 million U.S. consumers have already been transitioned away from screen scraping to a version of the FDX API.

In a little over two years, FDX has delivered key standards, guidelines and best practices into the marketplace. The following are the key FDX deliverables to date and those anticipated in the near future:

- FDX API Specification: Currently at version 4.5, the FDX API offers the ability to access over 500 different financial data elements, including banking, tax, insurance, and investment data, making it one of the most comprehensive Open Finance standards in the world. The FDX API utilizes foundational and globally interoperable standards for security, authentication, data transfer, authorization, API architecture, and identity and represents a global best-in-class solution set for user-permissioned data sharing.

- User Experience & Consent Guidelines: The User Experience and Consent Guidelines are intended to accelerate design decision-making during implementation of data sharing experiences. The guidelines specify what information and control must be given to consumers to ensure consistent data sharing experience regardless of where their data is held or who they are seeking to share it with.

- Taxonomy of Permissioned Data Sharing: In an effort to align industry stakeholders and help regulators and policymakers better understand and define the various roles and perspectives within the user-permissioned financial data ecosystem, FDX maintains a set of common terminology to be used as a taxonomy for the ecosystem. This documentation also includes a conceptual flow model to show how consumers interact with different participants within the current ecosystem that is evolving from legacy to new technology.

- Use Cases: Use cases are consumer-permissioned scenarios that help users minimize the amount of data they share by defining only the data elements that are needed for a given product or service. FDX use cases allow the financial services ecosystem to identify appropriately minimized and certifiable data sets needed to power an application and then utilize an industry-led standard like the FDX API to deploy and increase adoption of these use cases. So far, FDX has approved a Personal Financial Management (PFM) use case and expects to define and certify other specific use cases in the future, such as credit management and servicing, account verification, tax preparation and others.

- Developing a Certification Program: A qualification and certification program is needed to ensure common implementation and interoperability of any technical standard. Products (i.e., programs and applications that leverage consumer-permissioned financial data sharing) can be approved by a certification program to test the technical compatibility/interoperability, prior to being marketed as a compliant product, or getting access to certain intellectual property rights. Work continues on FDX's certification platform, and FDX recently released foundational requirements covering availability, performance, and security that implementations of the specification must meet to apply for a FDX use case certification.

- Global Registry: FDX envisions the creation of a registry of trusted organizations in order to help the user-permissioned financial data marketplace clearly identify ever-evolving technologies and new market entrants, as well as the web of often proprietary, incomplete, and incompatible technical standards that complicate the market today. Such a registry will enable those operating within the FDX ecosystem and other ecosystems to reliably identify and verify trusted organizations. In addition, FDX envisions that the registry will provide assurance regarding reliability and performance of data, traceability, transparency and trust in the FDX certification. FDX intends the Global Registry to act as a non-profit, non-commercial, technology agnostic, multi-tenant, cross-sector, international resource.

The work being done by FDX has the benefit of further enhancing competition and innovation in financial services. A common, interoperable, royalty-free, market led standard that has broad stakeholder support provides foundational requirements for entities seeking to serve the market for user-permissioned data sharing. Further, FDX as a non-profit industry standards body also provides large incumbents and small start-ups alike with a level playing field on which to compete.

c. Akoya

While the development of API standards such as those developed by FDX play a critical role, standards still need to be implemented through actual API connectivity. Without the creation of a central utility, each data holder needs to establish individual connectivity with each data aggregator or data user. This one-to-one model, which would require a plethora of individual and potentially differently configured connections across the ecosystem, can be made more efficient for data aggregators, data users, and data providers alike. Akoya provides an option that solves for the inefficiencies of this model by providing a one-to-many architecture, whereby each data holder can reach any Akoya connected data aggregator or data user through a single API connection with the central utility, Akoya. Data aggregators, data users and data holders alike all have the opportunity to benefit from only integrating once with the Akoya Data Access Network in order to be able to securely exchange consumer-permissioned financial data with one another. The efficiency offered to the market by Akoya may be particularly beneficial to smaller financial institutions and their third-party service providers as they seek to implement API-based data sharing capabilities.

In addition, Akoya facilitates the control, transparency, safety and security that the Bureau envisions being present in the data aggregation space. Consumers using Akoya never give out their user names and passwords (or credentials) and instead login directly with their data holder to authenticate and then grant access to a data aggregator or data user. Further, Akoya is fully compliant with the FDX API specification and does not retain any of the data that passes through the network. Members of the

Akoya Data Access Network receive web applications that provide documentation, reports and information on data elements that are being accessed and the products that are accessing them. Consumers can review, update, and revoke data access to their authorized entities through an interface provided within their existing digital experience at the FI data holder.[26] These qualities, which have been built into Akoya since its inception, fully align with the Bureau's Principles and allow Akoya to serve as a model reference for how the Bureau has envisioned consumer permissioned data access will be implemented in a manner that puts consumer interests at the forefront.

III. Requirements of DFA § 1033

The touchstone of any further action the Bureau may take to address authorized data access[27] must start with an analysis of the requirements of Section 1033, which establishes a consumer's right to access certain information.[28] While Section 1033 sets forth important rights, it also contains important limitations. Specifically, the statute requires the transmission to permissioned parties of data only – it does not require that covered persons enable permissioned parties to make changes to the data while it is in the control or possession or a covered person (data aggregators and data users are free to change the data one it is in their possession) or enable transactional processes that may be initiated by the data recipient.[29] Second, it requires that data access must be "request[ed]" by a consumer.[30] Third, the information must be in the "control or possession" of the covered person and must concern a "product or service" obtained from the covered person.[31] Importantly, Section 1033 does not impose any duty to keep or maintain *specific* information or to create information, it only requires the provision of what is already otherwise in the control or possession of the covered person.[32] Finally, Section 1033 requires data to be made available in an electronic form "usable by consumers" generally – specific or one-off formatting is not required.[33]

Section 1033 also contains a number of important exceptions. A covered person is not required to make available to the consumer (or a permissioned third-party):

- Confidential information, including an algorithm used to derive credit scores or other risk scores or predictions;
- Information collected by the covered person for the purpose of preventing fraud or money laundering or detecting or making any report regarding other unlawful or potentially unlawful conduct;

---

[26] Additional information about Akoya and the Akoya Data Access Network is available at: https://akoya.com/ (accessed Jan. 7, 2021).

[27] The Bureau has defined "authorized data access" as "third-party access to consumer financial data pursuant to the relevant consumer's authorization." 85 Fed. Reg. 71,003, at 71,004.

[28] Specifically, a "covered person" must "make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or the account, including costs, charges and usage data." The statute further specifies that "[t]he information shall be made available in an electronic form usable by consumers." *See* 12 U.S.C. § 5533(a).

[29] In data processing parlance, the requirements set forth in § 1033 are "read only, not write."

[30] *See* 12 U.S.C. § 5533(a) (providing for information to be made available "upon request").

[31] *Id.*

[32] *See id*. at § 5533(c) (providing that "[n]othing in this section shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer.")

[33] *See* 12 U.S.C. § 5533(a).

- Any information required to be kept confidential by any other provision of law; or
- Any information that the covered person cannot retrieve in the ordinary course of its business.[34]

Section 1033 requires the Bureau to address standardized formats for data. Fundamentally, however, the statute does not direct the Bureau to promulgate standardized formats for the exchange of information itself, but, rather, to "prescribe standards applicable to covered persons to *promote* the development and use of standardized formats for information…."[35] The statute therefore envisions that the Bureau would pursue a principles-based approach that would provide high-level guidance pursuant to which private sector standard setting bodies like the Financial Data Exchange (FDX) could develop and maintain detailed market-driven standards to facilitate the information exchange required by Section 1033. For the reasons more fully set forth herein, TCH believes that a market-driven approach to the development and maintenance of standards is far preferable to a regulatory one.

Finally, Section 1033 requires the Bureau to consult with the Federal banking agencies and the Federal Trade Commission to ensure that rules prescribed by the Bureau under Section 1033 impose substantively similar requirements on covered persons, take into account conditions under which covered persons do business in the U.S. and other countries, and not require or promote the use of any particular technology in order to develop systems for compliance.[36] TCH believes that such consultation is essential. A number of Federal banking agencies have already developed requirements (or signaled that they may develop requirements) relating to data sharing and data aggregation activities. Those efforts and other requirements that apply to the financial services sector must be taken into account in any further action the Bureau may take. Further, for any solution to scale, uniform requirements must exist across the industry in order to avoid having to bifurcate solutions.

IV. *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*

In October of 2017 the Bureau released the Principles in order to "reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data."[37] The Principles were intended to express the Bureau's vision for "realizing a robust, safe and workable data aggregation market that gives consumers protection, usefulness, and value" and the Bureau noted that "a common understanding of consumer interests is essential so that effective consumer protections can be integrated consistently into … [the] market."[38] TCH and its member banks fully support the Principles and have made significant progress in the intervening years to implement the Bureau's vision. TCH and its member banks fully agree with the Bureau that "consumer interests must be the priority of all stakeholders as the aggregation services-related market develops."[39]

---

[34] *See* 12 U.S.C. § 5533(b).
[35] *Id.* at §5533(d) (emphasis added).
[36] *Id.* at §5533(e).
[37] "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," *supra* note 5, at 1.
[38] *Id.*
[39] *Id.*

While much progress has been made in furthering the development of a safer and more secure, transparent, and consumer-centric market for aggregation services, TCH agrees with the Bureau that "there are indications that some emerging market practices may not reflect the access rights described in section 1033."[40] Further, while significant steps have been taken to realize the Bureau's vision as set forth in the Principles, some market practices do not reflect the Bureau's fundamental vision for data sharing and the importance of a consumer-centric approach with appropriate consumer controls and protections. TCH believes that many of the answers to questions posed by the Bureau in the ANPR can be deduced from an analysis of the Principles and an examination of existing market practices and initiatives, and whether those market practices and initiatives are likely to be able to achieve, absent further action by the Bureau, the desired state that the Principles outline. Each of the Principles is examined below.

a. *Principle 1 - Access. Consumers are able, upon request, to obtain information about their ownership or use of a financial product or service from their product or service provider. Such information is made available in a timely manner. Consumers are generally able to authorize trusted third parties to obtain such information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner.*

   Financial account agreements and terms support safe, consumer-authorized access, promote consumer interests, and do not seek to deter consumers from accessing or granting access to their account information. Access does not require consumers to share their account credentials with third parties.

Significant progress has been made on developing a framework for data sharing that aligns with the Bureau's vision as outlined in Principle 1. The work being done by the industry through FDX provides the necessary standard by which Consumers can more safely and securely obtain information from account providers to use for the consumer's benefit without requiring consumers to share their account credentials with third parties. Further, work being done by TCH and Akoya is geared toward accelerating the adoption of the FDX standard and more fully building out the industry infrastructure needed to support it.[41] Fundamentally, TCH believes that the Bureau should continue to rely on private sector market-led efforts for technical standard setting of the kind engaged in by FDX and believes it would be a mistake for the Bureau to attempt to define technical standards in any way. Regulatory-led or government mandated technical standards related to financial data sharing would necessarily be limited in scope, time consuming and unable to adapt quickly to market conditions and technological changes and have the potential to significantly slow or freeze innovation. Further, Section 1033 does not charge the Bureau with the development of technical standards itself, but, rather with taking action to "promote the development and use of standardized formats for information…."[42]

[40] 85 Fed. Reg. 71,003.

[41] Much of the work being done by TCH and Akoya is geared to addressing issues that will be faced by smaller institutions in implementing API environments. TCH's Assessment Tool created efficiencies relating to due diligence and third party risk management. Akoya created efficiencies relating to connectivity and is also working on the development of a rule set that may substantially alleviate the burdens of bilateral contracting. TCH further recognizes that third party service providers, which provide much of the back office infrastructure for smaller FIs, will also play a critical role in API adoption.

[42] *See* 12 U.S.C. § 5533(d) (emphasis added).

There are a number of actions that the Bureau could take that would be consistent with the Bureau's charge in Section 1033. First, TCH encourages the Bureau to find ways to explicitly endorse or reference technical standards and certification organizations like FDX and the work that they are doing.[43] Second, as more fully set forth herein, there are a number of issues on which the CFPB could provide greater regulatory clarity, allowing the industry to then work together to develop or further enhance existing standards to implement the CFPB's vision. Finally, the CFPB should work with other regulators to ensure that the Federal financial regulators are speaking with one voice on issues affecting the data aggregation market.[44]

While much progress has been made in developing standards and infrastructure to facilitate the movement from credential-based data access and screen-scraping to APIs, credential sharing and credential storage as well as screen scraping continue to be predominant practices in the market. Credential sharing and credential storage pose significant risks to consumers, including risks related to data breaches and fraudulent and unauthorized transfers as well as identity theft and other data privacy issues, and should be abolished. There may, however, be little incentive for data aggregators and data users to halt these practices given that the alternative of obtaining the data through APIs offers more limited, consumer controlled and transparent data access, that API access will necessarily subject data aggregators and data users to some level of risk management due diligence,[45] and that API access will impose certain costs associated with building and maintaining API connectivity. If the Bureau is going to engage in a rulemaking, then there would be substantial consumer benefits in hastening the transition away from credential based data access and screen scraping and to more secure methods like APIs, including more transparency to consumers about who is accessing their data, who is authorized, protecting consumer data from fraud or theft, and having data that is more timely and accurate than that obtained via non-API methods. Such action could take the form of the Bureau articulating a rule

---

[43] Once such example of endorsement of a market-led standard is the Financial Stability Oversight Council's (FSOC) annual report in which FSOC recommended that member agencies support adoption and use of standards in mortgage data, including consistent terms, definitions, and data quality controls. The recommendation pointed to the Mortgage Industry Standards Maintenance Organization (MISMO). (*See* "2020 Annual Report," Financial Stability Oversight Council, pp. 13 (Dec. 4, 2019) (available at: https://home.treasury.gov/system/files/261/FSOC2020AnnualReport.pdf (accessed Jan. 7, 2021)).

[44] TCH notes, for example, that the FDIC recently gave some indication that it may be proceeding down a separate path to address due diligence activities in which its banks may be engaged relating to data sharing and other fintech relationships. (*See*, *for example*, "Conducting Business With Bank[,] A Guide For Fintechs and Third Parties," FDIC, at pp. 2-5 (Feb. 2020) (describing due diligence obligations of banks and how banks conduct due diligence in advance of working with third parties) (available at: https://www.fdic.gov/fditech/guide.pdf (accessed Jan. 7, 2021)); "Banking With Apps," FDIC (Dec. 7, 2020) (distinguishing FDIC-insured banks from other entities) (available at: https://www.fdic.gov/resources/consumers/consumer-news/2020-11.html (accessed Jan. 7, 2021)); *and* "FDIC Seeks Input on Potential Voluntary Certification Program to Promote New Technologies," FIL-71-2020 (July 20, 2020) (seeking input on a proposal to promote the adoption of financial technology through, in part, a voluntary certification or assessment program that "could support financial institutions' due diligence of third-party providers of a range of technology and other services…") (available at: https://www.fdic.gov/news/financial-institution-letters/2020/fil20071.html (accessed Jan. 7, 2021)) (published in the Federal Register at 85 Fed. Reg. 44,890 (July 24, 2020))). Such initiatives, to the extent they result in different requirements for differently chartered financial institutions, have the potential to bifurcate the market and introduce challenges to the scalability of any given solution.

[45] *See* "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," Office of the Comptroller of the Currency (March 5, 2020) (at FAQs ## 4-7, describing agreements for sharing customer-permissioned data through APIs and risk management due diligence requirements) (available at: https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html (accessed Jan. 7, 2021)).

that prohibits a data aggregator or data user from obtaining consumer data using a consumer's online banking credential and screen scraping where a data holder has provided the data aggregator or data user with the option of enabling API access under fair and reasonable terms. The Bureau may also wish to consider a rule that sunsets credential based data sharing, storage and screen scraping upon a schedule that would be phased in over time by institutional size.

Further, as the Bureau notes in Principle 1, the purpose for which data access is given should be limited to "use on behalf of consumers, for consumer benefit." Consistent with this language, the Bureau in any rulemaking should clarify that data access is limited to circumstances in which a data user will provide services to the consumer that is providing the data, reasonably requires the data to provide those services and does so in a way that is transparent and consistent with consumer expectations.[46] If data is sold to third parties for use in research or analytics unrelated to the underlying service, that information should be clearly and conspicuously disclosed to consumers and subject to their consent.[47] Enforcement of these requirements would require supervisory oversight from the Bureau. FI data holders are not positioned and should not be expected to know and be able to police downstream uses of data.

There is also a need for the Bureau, if it is going to engage in a rulemaking, to further elaborate on the concept of a "trusted third party" that is contained within Principle 1.[48] TCH believes that the concept of trusted third party should require trust by both the consumer *and* by the data holder. As TCH's consumer research shows, consumers often have little understanding of the terms and conditions of the services they sign up for, how their data will be used, and who their data will be shared with.[49] As more fully set forth below, greater transparency on all of these issues is key to ensuring appropriate consumer "trust" in any given third party. FI data holders also have regulatory expectations relating to safety and soundness that they must fulfill in providing consumer data to data aggregators and data users.[50] These regulatory expectations make clear that FIs must conduct appropriate risk management

---

[46] For example, a consumer that signs up for a loan generating application that accesses their FI data as part of the application process would not reasonably expect their data to continue to be accessed after the application is completed and sold for other purposes. Similarly, a consumer signing up for services from a P2P payments application that accesses their account number and routing data to effectuate the payment would not reasonably expect their transactional data and other account information to be accessed and used for other purposes.

[47] *See, e.g.,* Letter to the Hon. Joseph J. Simons, Chair, Federal Trade Commission, from Senators Ron Wyden, Sherrod Brown and Representative Ann Eshoo (Jan. 17, 2020) (requesting that the FTC investigate Envestnet, Inc., the operator of Yodlee, regarding its sale of consumer data to data brokers, noting that "Envestnet does not inform consumers that it is collecting and selling their personal financial data") (available at: https://www.wyden.senate.gov/imo/media/doc/011720%20Wyden%20Brown%20Eshoo%20Envestnet%20Yodlee%20Letter%20to%20FTC.pdf (accessed Jan. 19, 2021)).

[48] "Consumers are generally able to authorize *trusted third parties* to obtain such information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner." ("Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," *supra* note 5, p. 3 (emphasis added).)

[49] *See* "Consumer Survey: Financial Apps and Data Privacy," *supra* note 31, pp. 2-3 & 5 (noting that many consumers who claim to have read terms and conditions do not understand what they've read).

[50] *See*, *for example,* "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (April 2016) (setting forth standards for protecting the security, confidentiality, and integrity of FIs' customers' information) (available at: https://www.fdic.gov/regulations/laws/rules/2000-8660.html (accessed Jan. 7, 2021)); "Third-Party Relationships: Risk Management Guidance," *supra* note 30 (requiring bank management to evaluate and manage risks associated with third-party relationships and "avoid excessive risk taking that may threaten a bank's safety and soundness"; *and* "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," *supra* note 41, at FAQ # 4 (noting that "screen-scraping can pose operational and reputation

due diligence and, based on that due diligence, make an appropriate risk management decision in order for such data sharing to take place. Accordingly, in any rulemaking the Bureau undertakes it should clarify that the concept of a "trusted third party" requires trust not only by the consumer, but also requires that the data aggregators and data user will have satisfactorily met the FIs own reasonable risk management criteria in order to qualify.[51] Such requirements must include not only appropriate information security controls, but also insurance and financial requirements that are commensurate to the risks being introduced.

Any rulemaking engaged in by the Bureau should also clarify an FI's ability to control access, affirm authentication and impose reasonable time, place, and manner restrictions in circumstances that are consistent with protecting the consumer and the safety and soundness of the financial system. This should include any circumstances in which the FI has a good faith belief that access may be fraudulent, may present security risks to the consumer, the FI, or the financial system generally, may relate to misuse of the consumer's data, or may relate to data beyond that which is reasonably related to the product or service being provided to the consumer or as reasonably needed to protect the security, efficiency, and operational integrity of the FI data holders own systems.[52] Because FIs hold much of the liability relating to unauthorized transfers and all of the costs of recredentialing consumers in the event of fraud or unauthorized access, FI data holders have legitimate interests and an appropriate role to play in protecting their customers and protecting the safety and soundness of the financial system.

Finally, if the CFPB engages in a rulemaking then the CFPB should ensure that it includes certain actions that would greatly enhance the ability of consumers and FIs to "trust" third parties. Many of the issues related to data aggregation can be traced to the problem of consumer data leaving the highly regulated, supervised, and examined financial institution environment and, in many cases, entering a much more lightly regulated fintech environment that often is not subject to any supervision and examination.[53] The CFPB has the authority to provide such supervision and examination pursuant to its larger participant rulemaking authority in Section 1024(a)(1)(B) or pursuant to its authority under

---

risks" and that banks "should take steps to manage the safety and soundness of the sharing of customer-permissioned data with third parties"). *See also* Federal Financial Institutions Examination Council, "Outsourcing Technology Services" IT Examination Handbook, p. 25 (noting that supervised institutions should ensure that service providers can maintain the confidentiality of customer data and possess sufficient controls to "ensure the security and confidentiality of information assets consistent with the institution's information security program) (June 2004) (available at: https://ithandbook.ffiec.gov/media/274841/ffiec_itbooklet_outsourcingtechnologyservices.pdf (accessed Jan. 7, 2021)).

[51] Such risk management criteria should be limited to the FI providing a physical connection for data transmission that it believes to be secure. The Bureau should recognize that the third or fourth party is acting as an agent of the FI's customer and that the FI will have limited to no control over data usage and practices once the data leaves the FI.

[52] Any such clarification, however, must also recognize that such action on the part of the FI data holder may not always be feasible. FI data holders may not always be able to identify third-party use of a customer's credentials and screen scraping given that technology on both the FI data holder and data aggregator / data user sides is rapidly evolving.

[53] While the FTC has "after the fact" enforcement authority, such authority is not an appropriate substitute for robust supervision and examination, particularly when data users are increasingly engaged in bank-like activities and are engaged in handling the same kinds of sensitive consumer information that banks have traditionally been trusted to safeguard.

Section 1024(a)(1)(c).[54] In order to ensure an appropriate trust environment, any rulemaking by the CFPB should include appropriate supervision and examination of data aggregators with appropriate requirements for data aggregator due diligence and oversight of data users with whom consumer information is shared.

b. Principle 2 – Data Scope and Usability. Financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards. Information is made available in forms that are readily usable by consumers and consumer-authorized third parties. Third parties with authorized access only access the data necessary to provide the product(s) or services(s) selected by the consumer and only maintain such data as long as necessary.

TCH submits that achievement of the Bureau's vision as outlined in Principle 2 may be inhibited because this is an area in which incentives may not be properly aligned. Data aggregators and data users that are engaged in screen scraping are currently obtaining data well-beyond that which may be needed to provide a consumer with any particular service (and likely well-beyond what a consumer may believe they have agreed to share). Absent a mandate, there may not be adequate incentive to transition beyond screen scraping to a more controlled API environment where only data required to provide the consumer with the service is being shared.

Second, the use cases being developed by FDX are quite broad and individual services that are within the overall FDX use case may actually have a much narrower need for data. Regardless of the technical standard, there would be a need for the Bureau in a rulemaking to clarify that the standard must be subservient to an overall data minimization principle – that a data aggregator or data user should still only obtain and use data strictly as needed for the service currently being provided, and, further, that the consumer should be fully in control of what categories of data are being provided, to whom, for how long, and for what purpose regardless of use case.

Third, consumers can only be assured that a service is only accessing the data necessary to provide the service and only maintains the data as long as necessary if there is adequate transparency as to the nature of the service, what data is being accessed, for what use, by whom, and for how long. As is more fully noted in Appendix I, a survey of existing terms and conditions shows that this level of transparency is not generally being provided.[55] If the Bureau is going to engage in a rulemaking, then it

[54] Pursuant to 12 U.S.C. § 5514 (a)(1)(B), the Bureau has the authority to supervise larger participants of a market for consumer financial products or services as defined by rule. In addition, the Bureau has the authority under 12 U.S.C.§ 5514(a)(1)(C) to supervise any covered person that is engaged or has engaged in conduct that poses risks to consumer with regard to the offering or provision of consumer financial products or services. Given the risks attendant to handling consumer data, the Bureau should exercise this authority.

[55] Such concerns were echoed by the CFPB Taskforce, which noted in its Report that "[a]lthough data aggregators obtain a consumers' consent before accessing or using data about the consumer, widespread concern exists that (1) consumers do not provide *meaningful* consent, and (2) data aggregators obtain more data, and retain it longer, than necessary to provide their product or service." (*Id.* at pp. 512-513). The Taskforce also notes that "[s]takeholders have also highlighted concerns that data aggregators' user agreements are often unclear or silent about how consumers can opt out of data collection" and that agreements often "state that the company will not store the consumer's account credentials or other information, but [] fail to disclose that the FinTech company will use a third-party data aggregator and that the aggregator will retain the consumer's credentials and other data";

should address this issue. Data aggregators and data users should be required to disclose the identity of each data aggregator or data user to which a consumer's data is being provided and each data user with whom information is shared should be required to obtain a separate and distinct authorization from the consumer. If data is sold to third parties for use in research or analytics unrelated to the underlying service, that information should be clearly and conspicuously disclosed to consumers and subject to their consent. This is consistent with consumers' desire to have more transparency and control over the use of their information and comports with standards being implemented elsewhere in the fintech space. [56] Importantly, this level of disclosure and control will only be able to be provided at the application level. FI data holders will not generally be in possession of information relating to the downstream uses of the consumer's data

Fourth, any action taken by the Bureau should recognize the limitations imposed by Section 1033. Specifically, the exceptions that are set forth in the statute for the following:

- Confidential information, including an algorithm used to derive credit scores or other risk scores or predictions;
- Information collected by the covered person for the purpose of preventing fraud or money laundering or detecting or making any report regarding other unlawful or potentially unlawful conduct;
- Any information required to be kept confidential by any other provision of law; or
- Any information that the covered person cannot retrieve in the ordinary course of its business.

These exceptions raise several issues. Specifically, clarity is needed on the nature and extent to which confidential information may be protected from disclosure. TCH believes that the protection for confidential information should include commercially sensitive trade secrets that are not otherwise disclosed to consumers. This protection should extend to the use of artificial intelligence and other methods by data aggregators or data users to reverse engineer such trade secrets based on the extraction of large quantities of consumer data. Interest rates, account fees, and other terms under which services are provided to consumers and offers made to individual consumers that are disclosed to them are certainly subject to disclosure under Section 1033. There should be a distinction, however, between the disclosure of information made available to a particular consumer and the use of big data to reverse engineer proprietary algorithms and other proprietary processes used by a data holder to conduct its business. Notably, prohibiting such reverse engineering would be similar to the prohibition frequently found in data aggregator and data user agreements that prohibit those accessing *their* services from using the data they provide to reverse engineer their own proprietary systems and processes.[57] The Bureau in any rulemaking should clarify that such reverse engineering is not an

---

or that "user agreements also may omit terms regarding the duration of an aggregator's access to data, which can result in perpetual access unless the consumer affirmatively withdraws consent." (*Id.* at 513).

[56] Apple, for example, recently announced that it will be enhancing user privacy by removing apps from its App Store that track users without first receiving their permission. *See* CNBC, "Apple Executive Warns He Could Remove Apps That Track Users Without Permission" (Dec. 8, 2020) (available at: https://www.cnbc.com/2020/12/08/apple-may-remove-apps-that-track-users-without-permission-in-2021.html (accessed Jan. 7, 2021)).

[57] *See*, *for example,* Acorns, "Terms of Use," at "Permitted Uses" and "Prohibited Uses" (May 13, 2020) (prohibiting reverse engineering, de-compiling, or otherwise translating Acorns content or user interface material); MX, "TERMS OF USE," at "Limitations" (Jan. 15, 2020) (prohibiting, without express prior written consent, reverse engineering, decompiling, altering, modifying, disassembling, or otherwise attempting to derive source code used

appropriate use of the data for the purpose of providing the product or service selected by the consumer. In addition, information that is licensed by the FI under terms that prevent its disclosure to third parties should also fall within the category of confidential information that is excepted from disclosure.

Fifth, clarity is needed as to the extent to which the Fair Credit Reporting Act (FCRA) applies to permissioned data and what obligations, if any, are imposed on various stakeholders. TCH submits that FI data holders cannot and should not be subject to FCRA requirements relating to furnishers of information.[58] FI data holders are not in the position of actively providing the data, but rather are mere conduits for information that is being pulled by the data aggregator or data user acting as their customer's agent.[59] FI data holders will not generally know the purposes for which data is being pulled by a data aggregator or data user or how it may be manipulated, used, or displayed once it is out of the possession of the FI. Further, requiring FIs to take on the obligations of furnishers under FCRA has the potential to clash with the limitations of Section 1033, which require the FI to make available only that information that is in the "control or possession" of the FI and which specifically excepts "any information that the covered person cannot retrieve in the ordinary course of its business."[60] Section 1033 requires that a data provider disclose what it has and no more. Conversely FCRA may impose a duty on furnishers to create or manipulate the data in a way that makes it specifically usable for credit reporting purposes.

Finally, any standards, in order to be enforceable, will require appropriate supervision and enforcement by the Bureau through a larger participant rulemaking or other assertion of supervisory authority.

c. *Principle 3 – Control and Informed Consent. Consumers can enhance their financial lives when they control information regarding their accounts or use of financial services. Authorized terms of access, storage, use, and disposal are fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer. Terms of data access include access frequency, data scope, and retention period. Consumers are not coerced into granting third-party access. Consumers*

---

in MX services or any third-party applications incorporated into MX services); Plaid, "End User Privacy Policy," at "Control and Responsibilities" and "Prohibited Conduct" (Dec. 30, 2019) (providing that users agree not to modify, reverse engineer, or seek to gain unauthorized access to Plaid's platform or related systems, data or source code); *and* Venmo, "User Agreement," at "Licenses grants, generally" (Jan. 2, 2021) (providing that users agree not to engage in numerous activities, including reverse engineering or attempting to create any code derived from Venmo software or any third party materials or technology that are incorporated).

[58] *See* Kwamina Thomas Williford and Brian J. Goodrich, "Why Data Sources Aren't Furnishers Under Credit Report Regs," Holland & Knight (Sept. 25, 2019) (available at: https://www.hklaw.com/-/media/files/insights/publications/2019/09/whydatasourcesarentfurnishersundercreditreportregs.pdf?la=en (accessed Jan. 7, 2021)).

[59] Such a result is consistent with Regulation V, which specifically excepts disclosures by a consumer from the definition of a "furnisher" for purposes of FCRA. *See* 12 C.F.R. 1022.41 (c)(3) ("An entity is not a furnisher when it … [i]s a consumer to whom the furnished information pertains…." When a consumer directs an FI data holder to provide data to a data aggregator, the consumer should be the one viewed as ultimately providing the information to the data aggregator and/or lender data user, and the exception from the furnisher definition for consumers to whom the furnished information pertains should apply.

[60] 12 U.S.C. § 5533(a) and (b)(4).

understand data sharing revocation terms and can readily and simply revoke authorizations to access, use, or store data. Revocations are implemented by providers in a timely and effective manner, and at the discretion of the consumer, provide for third parties to delete personally identifiable information.

An analysis of the terms and conditions set forth in Appendix 1 shows that current disclosures provided by data aggregators and data users fall well short of the vision articulated by the Bureau in Principle 3. Absent greater transparency, consumers cannot exercise the level of control and informed consent that the Bureau envisions. While some work is being done by the industry through bilateral and model agreements as well as through FDX, including the development of user experience guidelines, TCH believes that the market alone will not be able to ensure that data aggregators and data users will provide consumers with the level of control, transparency and informed consent the Bureau envisions. If the Bureau is going to engage in a rulemaking, then a regulatory framework will be needed to address several issues. First, the framework should include disclosure requirements for all parties and should set forth model disclosures that create a safe harbor for various stakeholders. Such requirements should recognize that FI data holders will have limited visibility into data usage and downstream parties. Accordingly, data holders should generally be limited to disclosing to whom the data is initially being provided, the fact that the provision of data was authorized, and identification of the appropriate mechanism through which the consumer may halt the ongoing provision of data.

Disclosure obligations alone, however, will not fully address the issue of consumer control given downstream usage of consumer data unless the regulatory framework ensures that the control environment travels with the data. Therefore, an appropriate regulatory framework would need to ensure that data aggregators have reasonable risk management programs in place designed to oversee risks associated with data users, and that ensure that all downstream parties are known, that their use of data is disclosed to the consumer, that the consumer is clearly giving informed consent, and that data aggregators and data users have appropriate controls in place to safeguard the data, and to delete the data once consumer consent is revoked.[61]

A regulatory framework would also need to address authorization requirements with disclosures that are sufficiently clear and easily understood by consumers to ensure that authorization is knowingly given. Further, consumers often mistakenly believe that deleting the underlying application for the service using the consumer's data will stop the flow of data or may otherwise forget that they may have signed up for a particular service. For this reason, consumer control of the flow of data should be enabled at both the data holder and the data aggregator / data user. To assure that consumers continue to wish to provide their data, the regulatory framework would need provide for mandatory periodic affirmative reauthorization no less frequently than annually. Disclosures should also clearly spell out the consumer's right to revoke consent and should include the right to be forgotten. If the Bureau determines that the sale of consumer data unrelated to the direct provisions of a service is within the scope of permissible activities under Section 1033, then the Bureau should also impose in any regulatory framework it develops a heightened "clear and conspicuous" standard for consent relating to the sale of consumer data unrelated to the direct provision of any service to the consumer.

[61] For example, under the Gramm-Leach-Bliley Act, reuse and redisclosure obligations travel with the data and need to be adopted by parties that receive the data. (*See* 15 U.S.C. § 6802.) (S*ee also* 12 C.F.R. § 1016.11 (implementing this provision).)

To ensure meaningful compliance, any regulatory framework developed by the Bureau would need to require appropriate supervision and enforcement through a larger participant rulemaking or other assertion of supervisory authority.

d. Principle 4 – Authorizing Payments. Authorized data access, in and of itself, is not payment authorization. Product or service providers that access information and initiate payments obtain separate and distinct consumer authorizations for these separate activities. Providers that access information and initiative payments may reasonably require consumers to supply both forms of authorization to obtain services.

TCH agrees with the Bureau that authorized data access is not payment authorization and that payment authorization should require a separate and distinct consumer authorization. It should be noted, however, that Section 1033 defines only the terms of data access. While data that is provided pursuant to the terms of Section 1033 may be used by a provider to assist in the process of initiating a payment, payment authorization itself is beyond the scope of Section 1033 and defining what constitutes appropriate payment authorization will be governed by the requirements of other laws or payment system rules.[62]

It should also be noted that the movement of money carries heightened risks for consumers and for FI data holders relating to unauthorized payments and fraud.[63] Accordingly, FI data holders may have heightened requirements for the disclosure of information that can be used to initiate payments, including the imposition of enhanced security measures such as tokenization, and the Bureau in any regulatory framework it develops should affirmatively recognize the legitimacy of such requirements.[64]

While TCH believes that the specific requirements relating to payment authorization are appropriately addressed by existing laws and payment system rules, TCH also believes that if the Bureau is going to engage in a rulemaking then consumers and the market would benefit from the Bureau including a rule that differentiates authorized data access pursuant to Section 1033 from payment authorization, and which recognizes that data holders may impose reasonable, heightened requirements (such as tokenization, heightened due diligence, increased security standards) for the provision of information that can be used to initiate payments. To ensure meaningful compliance, any

[62] Specifically, Section 1033 requires the transmission to permissioned parties of data only – it does not require that "covered persons" enable permissioned parties to make changes to the data or enable transactional processes that may be initiated by the data recipient.

[63] Under certain circumstances FIs may bear the risk of unauthorized payments and may be required to make consumers whole even though the unauthorized payment was initiated by a third party. In addition, FIs typically bear all the costs associated with recredentialing where such actions are necessary to prevent further instances of fraud.

[64] Such enhanced requirements are consistent with approaches taken in other jurisdictions, such as the UK, where companies wishing to enable payment initiation are subject to heightened compliance standards, including enhanced licensing, capital and insurance requirements. (*See* Financial Conduct Authority, "Account Information and Payment Initiation Services" (Aug. 12, 2017) (available at: https://www.fca.org.uk/consumers/account-information-and-payment-initiation-services (accessed Jan. 7, 2021)); *and* "Apply to Become an Electronic Money or a Payment Institution" (Jan. 15, 2015) (available at: https://www.fca.org.uk/firms/apply-emi-payment-institution (accessed Jan. 7, 2021)) (noting that Account Information and Payment Initiation Service Providers must be registered with the Financial Conduct Authority and meet additional requirements).)

regulatory framework developed by the Bureau would require appropriate supervision and enforcement through a larger participant rulemaking or other assertion of supervisory authority.

> e. *Principle 5 – Security. Consumer data are accessed, stored, used, and distributed securely. Consumer data are maintained in a manner and in formats that deter and protect against security breaches and prevent harm to consumers. Access credentials are similarly secured. All parties that access, store, transmit, or dispose of data use strong protections and effective processes to mitigate the risks of, detect, promptly respond to, and resolve and remedy data breaches, transmission errors, unauthorized access, and fraud, and transmit data only to third parties that also have such protections and processes. Security practices adapt effectively to new threats.*

TCH believes that the security envisioned by the Bureau cannot adequately be achieved through market forces alone – regulatory action by the Bureau is needed. While Federally chartered banks are subject to detailed Federal Financial Institutions Examinations Council (FFIEC) guidance on information security and the interagency rules implementing Gramm Leach Bliley and, more importantly, supervision and enforcement by the Federal financial regulatory authorities, data aggregators and fintech data users that sit underneath them are, at most, subject to the much less stringent FTC safeguards rule[65] and, in most instances, no regulatory supervision and only after the fact enforcement by the FTC.[66] Even state chartered FIs are required to comply with detailed security measures and will be subject to state regulatory supervision and enforcement actions. Those regulatory frameworks are key to protecting consumers and preventing data breaches, transmission errors, unauthorized access and fraud, all of which are fundamental concerns that go to the heart of data sharing activities.

The security of consumer data has been the subject of considerable concern by Congress and other regulatory agencies, which have focused on the perceived misuse of consumer data by numerous fintech companies.[67] Similarly, the Facebook/Cambridge Analytica scandal shows that even with appropriate contractual limitations in place, absent robust third party risk management processes and

---

[65] As the CFPB Taskforce notes in its Report, there is significant uncertainty as to whether data aggregators and data users are "financial institutions" subject to GLBA and the Safeguards Rule. *See* CFPB Taskforce Report, Vol 1 at pp. 513-514.

[66] *See* Federal Trade Commission, "Standards for Safeguarding Customer Information" (codified at 16 C.F.R. Part 314) (notably, the FTC safeguards rule contains general requirements that are less detailed than the requirements provided under the Gramm-Leach-Bliley Act (differences between the two sets of requirements include standards regarding board and management involvement, employee background checks, vendor oversight, authentication, and incident response programs)). *See also* 81 Fed. Reg. 61,632 (Sept. 7, 2016) (requesting public comments on the standards for safeguarding customer information, including comment on whether a response plan should be a required element of an information security program).

[67] *See*, *for example*, NPR, "Amazon, Tik Tok, Facebook, Others Ordered to Explain What they Do With User Data (Dec. 15, 2020) (available at: https://www.npr.org/2020/12/15/946583479/amazon-tiktok-facebook-others-ordered-to-explain-what-they-do-with-user-data (accessed Jan. 7, 2021)); Lauren Feiner, "Big Tech Testifies: Bezos Promises Action if Investigation Reveals Misuse of Seller Data, Zuckerberg Defends Instagram Acquisition," CNBC (Dept. 8, 2020) (available at: https://www.cnbc.com/2020/07/29/tech-ceo-antitrust-hearing-live-updates.html (accessed Jan. 7, 2021)); Elizabeth Dwoskin, "Facebook is Accused of Digital 'Surveillance' Against Its Competitors," The Washington Post (July 29, 2020); *and* Michael Grothaus, "How Our Data Got Hacked, Scandalized, and Abused in 2018," Fast Company (Dec. 13, 2018) (available at: https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018 (accessed Jan. 7, 2021)).

appropriate supervision and enforcement the security of data cannot be assured.[68] In the context of data sharing under Section 1033, the data at issue, dealing with a consumer's financial information and often including PII, is even more sensitive than generalized consumer data and its distribution and use should be subject to heightened concern.

While FI data holders that are national banks have due diligence requirements imposed by the OCC and can play some role in ensuring that data aggregators incorporate security standards related to their API connectivity with banks, FI data holders have no relationship with most data users and as such those requirements should not extend to downstream activities. Only the data aggregators that contract with the data users are positioned to ensure appropriate security standards are in place for a data user accessing data via the data aggregator. Further, not all FI data holders have the wherewithal to perform such due diligence on data aggregators and, more importantly, no FI, regardless of size, will be able to address security practices at the thousands of fintech data users that comprise data aggregator clients. Further, while FIs may attempt to address security issues in bilateral agreements, such agreements must be individually negotiated and data aggregators have a powerful default position to simply continue credential-based access and screen scraping if the FI attempts to impose requirements that the data aggregator does not wish to incorporate.

Given data aggregator and data user access to similarly sensitive information, data aggregators that are the recipients of such information should be subject in any CFPB rulemaking to functionally similar requirements as those imposed on FIs, including supervision and enforcement that the CFPB should provide through a larger participant rule or otherwise.[69] In order to ensure a fully secure ecosystem, such requirements should follow the data with data aggregators being responsible for passing on and enforcing security requirements to data users.

f. Principle 6 - Access Transparency. Consumers are informed of, or can readily ascertain, which third parties that they have authorized are accessing or using information regarding the consumers' accounts or other consumer use of financial services. The identity and security of each such party, the data they access, their use of such data, and the frequency at which they access the data is reasonably ascertainable to the consumer throughout the period that the data are accessed, used or stored.

TCH's consumer research shows that consumers want increased control over the use of their data, consistent with the vision the Bureau has outlined in Principle 6. Unfortunately, as set forth in Appendix 1, data aggregators and data users are not, as a general rule, providing this level of specificity and consumers are not being afforded the level of transparency and control that the Bureau has set forth in Principle 6.

---

[68] *See* Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," The New York Times (April 4, 2018) (available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (accessed Jan. 7, 2021)); *and* Paolo Zialcita, "Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal," NPR (Oct. 30, 2019) (available at: https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal (accessed Jan. 7, 2021)).

[69] Such supervision would necessarily include supervision over the data aggregators' third party risk management program pursuant to which the data aggregator would be responsible for evaluating and managing risks associated with its data user customer's use of consumer data.

TCH does not believe that the market alone can achieve the vision outlined by the Bureau in Principle 6. If the Bureau is going to engage in a rulemaking then it should ensure that data aggregators and data users are providing consumers with the transparency and control that they need. Further, because FI data holders will generally have limited to no visibility into downstream activities, such transparency obligations generally may only be fulfilled fully by data aggregators and data users and the Bureau should as part of such rulemaking mandate their disclosure of such information such that each data aggregator and each data user make readily available to consumers what data they are accessing, how frequently they are accessing it, and for how long they are storing it.[70] TCH believes that the Bureau in any rulemaking should also make allowance for FIs to obtain data usage information from data aggregators and data users so that they may voluntarily provide it to consumers if the FI has the ability to provide the consumer with a one-stop, aggregated view of the consumer's data usage.[71] Such an aggregated view is clearly beneficial to consumers (particularly those who may have deleted an app or data user and believe that flow of data has stopped) and should be encouraged by the Bureau where possible. This helps the consumer be an active participant in stewarding their data and also helps facilitate principle 7, below, if a dispute arises.

The Bureau should also recognize that transparency and control are fundamentally enhanced through movement of the industry to an API environment. APIs allow data holders to monitor and control data access, at least to the initial data recipient, and permit data holders to pass information on to consumers that can increase the consumer's knowledge of and control over their data usage. The cessation of credential-based access and screen scraping is therefore intimately linked to achieving the increased transparency and control that the Bureau envisions in Principle 6.

Finally, as with other requirements, in order to ensure meaningful compliance, any rule developed by the Bureau should require appropriate supervision and enforcement through a larger participant rulemaking or other assertion of supervisory authority.

---

[70] As the Bureau considers ways in which it can increase transparency for consumers, it may wish to consult Section 204 of the Credit Card Accountability, Responsibility, and Disclosure Act (CARD Act) as a possible model. The Card Act requires creditors to (a) establish Internet sites on which creditor agreements must be posted, (b) provide copies of such agreements in electronic format to the Federal Reserve Board, and (c) required the Board to establish and maintain on its Internet site a central repository of consumer credit card agreements so that such agreements are easily accessible and retrievable by the public. The Bureau could consider a similar framework to ensure that data aggregator and data user agreements are easily accessible and retrievable by consumers.

[71] *See*, *for example*, Well Fargo's Control Tower service, which provides customers with centralized access to and control over their card- and account-related information (information about the Control Tower services is available at: https://www.wellsfargo.com/online-banking/manage-accounts/control-tower/ (accessed Jan. 7, 2021)) *and* JPMorgan Chase & Co ("Chase") Security Center application that allows its customers to see (i) the financial apps that are accessing their accounts through Chase's API, (ii) the specific accounts being accessed, (iii) the specific account information being accessed, and (iv) the last time it was accessed. Chase's service also enables customers to turn off account access for particular applications or entirely (Natalie Williams (Chase), "Written Statement, Symposium on Consumer Access to Financial Records" (Feb. 26, 2020) (available at: Https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-accessfinancial-records/ (accessed Jan 7.2021). (Note that the name of the Chase application was changed from AccountSafe to Security Center at some point after the submission of William's written statement).

g. *Principle 7 – Accuracy. Consumers can expect the data they access or authorize others to access or use to be accurate and current. Consumers have reasonable means to dispute and resolve data inaccuracies regardless of how or where inaccuracies arise.*

FIs understand the importance of providing accurate information to their customers and are committed to doing so. TCH believes that it is important, however, to interpret the vision articulated in Principle 7 consistent with the statutory parameters set forth by Congress in Section 1033. Congress wisely sought to minimize the burdens imposed on data holders by specifying that that the obligation of data holders be limited to providing only that information that is in the "control or possession" of the data holder and further specifying that data holders would not be required to make available any information that the data holder could not retrieve in the "ordinary course of business."[72] Consistent with these important limitations, the Bureau in any rulemaking should interpret its vision for data accuracy consistent with data holders making available information that is subject to a FIs standard posting times and other procedures that the FI has adopted for data handling in the ordinary course of its business. Section 1033 does not require a data holder to develop new information, only that it make available to an authorized entity whatever data is otherwise ordinarily available to the consumer.

The Bureau must also recognize the practical limitations that data holders face in that they are unlikely to be in a position to understand, much less control, downstream uses of data that is being accessed by data aggregators and data users. All of the purposes for which data is being accessed will, in most cases, not be transparent to the data holder and data holders will not be in a position to control downstream manipulation, use, and display of the data. Data holders cannot, therefore, be guarantors that data accessed will be accurate and current for all purposes and in all circumstances and, indeed, Section 1033 imposes no such requirement.

With regard to dispute resolution, there is a significant delta between the dispute resolution processes and resources that FI data holders have in place versus those available at the typical data aggregator or fintech data user. FIs have substantial resources devoted to established call centers and other methods through which consumers can dispute and resolve issues and are regulated and supervised for compliance with regulatory requirements relating to dispute resolution.[73] Given the substantial resources and processes that FIs already have in place, FIs should not be required to reinvent the wheel to handle dispute resolution issues relating to data, but should be permitted to rely on their existing infrastructures.[74]

Conversely, consumers generally face a much different environment in any attempt to resolve issues with data aggregators and fintech data users. First, consumers may not even be aware that a particular fintech application is leveraging the services of a particular data aggregator or that a data aggregator has provided the consumer's data to a particular data user. Without a clear understanding of

[72] 12 U.S.C. §§ 5533(a) and (b)(4).

[73] For example, FIs already have detailed regulatory requirements under the Electronic Fund Transfer Act (EFTA)/Regulation E and the Truth in Lending Act (TILA)/Regulation Z for resolving disputes relating to unauthorized transfers and unauthorized credit card charges. (*See*, *for example,* 15 U.S.C. § 1693g(a)/12 C.F.R. § 1026.6 (limiting consumer liability for unauthorized funds transfers); *and* 15 U.S.C. § 1643(a)/12 C.F.R. § 1026.12(b)(1) (limiting cardholder liability for unauthorized charges to $50).)

[74] Further, as set forth on page 21, FI data holders cannot and should not be subject to FCRA requirements relating to furnishers of information.

the data aggregator's role or downstream flow of the data, a consumer will be powerless to resolve any dispute relating to the data aggregator or other data users' handling of the data. Second, many data aggregators and fintech data users have little to no dispute resolution infrastructure or process in place. Circumstances encountered by consumers dealing with a recent hack at Robinhood Markets are illustrative. Even in cases dealing with fraudulent transfers from Robinhood's accounts, circumstances that required an immediate and urgent response to prevent further fraud, consumers were faced with an "arduous process" dealing with a company that maintained "no support line for users to call for help, leaving customers to rely on emailed responses that can take weeks." [75]

In the clear absence of existing resources and processes, an appropriate dispute resolution infrastructure outlining minimum standards for data aggregators and data users commensurate with those already imposed on FI data holders will need to be a part of any regulatory framework that the Bureau adopts in implementing Section 1033. As with other requirements, in order to ensure meaningful compliance, any rule developed by the Bureau would require appropriate supervision and enforcement through a larger participant rulemaking or other assertion of supervisory authority

h. *Principle 8 – Ability to Dispute and Resolve Unauthorized Access. Consumer have reasonable and practical means to dispute and resolve instances of unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized data sharing access, and failures to comply with other obligations, including the terms of consumer authorizations. Consumers are not required to identify the party or parties who gained or enabled unauthorized access to receive appropriate remediation. Parties responsible for unauthorized access are held accountable for the consequences of such access.*

TCH acknowledges that there is significant overlap in the components that are required to address the Bureau's vision as outlined in Principles 7 and 8 and therefore reiterates its comments in Section IV(g), above. In addition, the issues present here are linked to those discussed in Principle 1. Fundamentally, as long as consumers are required to give out their login IDs and passwords to data aggregators and data users to facilitate data access and as long as screen scraping exists it will be substantially difficult if not impossible for FI data holders to resolve unauthorized access claims as the process of credential based access and screen scraping limits the FI data holder's visibility into what data is authorized and for whom. Tokenized access through an API is the only method through which an FI data holder can appropriately validate authorization and, therefore, the abolition of credential based access and screen scraping is fundamental to the achievement of the Bureau's vision as articulated in Principle 8. .

TCH also notes, as more fully discussed in Section IV(i), below, that FI data holders have clear regulatory requirements under Regulation E for the resolution of consumer disputes related to unauthorized payments.

i. Principle 9 – Efficient and Effective Accountability Mechanisms. The goals and incentives of parties that grant access to, access, use, store, redistribute, and dispose of consumer

[75] Sophie Alexander and Anders Melin, "Robinhood User Says $300,000 Restored From Hack, Then Taken Back," Bloomberg Wealth (Dec. 22, 2020) (available at: https://www.bloomberg.com/news/articles/2020-12-22/robinhood-user-says-300-000-restored-from-hack-then-taken-back (accessed Jan. 7, 2021)).

data align to enable safe consumer access and deter misuse. Commercial participants are accountable for the risks, harms, and costs they introduce to consumers. Commercial participants are likewise incentivized and empowered effectively to prevent, detect, and resolve unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized data sharing access, data inaccuracies, insecurity of data, and failures to comply with other obligations, including the terms of consumer authorizations.

The Bureau's vision as outlined in Principle 9 is unlikely to be achieved absent further regulatory action. Incentives amongst stakeholders are not properly aligned to achieve the Bureau's goals.

Data aggregators and data users may have little incentive to end credential-based access and screen scraping without a regulatory mandate to do so. The risks of credential-based access and screen scraping are largely borne by consumers and FI data holders. As shown in Appendix 1, existing terms and conditions imposed by data aggregators largely disclaim all or most responsibility for any loss that may result from data aggregator or data user activities. To the extent not accepted by data aggregators and data users, losses will be borne either by consumers or data holders. Consumers bear risks related to misuse of their data and data breaches, including identity theft, breach of privacy, and fraud. FI data holders hold the majority, if not all, of the liability that would accrue from a data breach or the unauthorized use of consumer data, including all of the cost of recredentialing the consumer to prevent further losses and potential liability for unauthorized transfers. Absent further regulatory action, data aggregators may opt to continue the status quo, particularly when one considers the costs of moving to an API environment, including submission to appropriate due diligence, the cost of connectivity, and the fact that the data that will be made available through APIs will be more narrowly tailored to appropriate use. Yet, as noted above, the industry's transition to APIs is fundamental to achieving much of the Bureau's vision for consumer protection, including enhanced safety, security, transparency and control over data usage.

If the Bureau engages in a rulemaking, then it should prevent data aggregators and data users from disclaiming liability to either the consumer or the data holder for acts or omissions relating to data while it is in their custody or control. Liability should follow the data and all parties should be fully accountable for its care.

Liability alone, however, is unlikely to lead to the appropriate implementation of the Bureau's vision. Both data holders and consumers may have challenges proving proximate cause – i.e., relating a particular data aggregator or data user's wrongful act to the damages suffered. Proximate cause issues can prove to be particularly difficult hurdles in data breach cases.[76] Additionally, many data users

[76] *See*, *for example*, Nicole Hong, "For Consumers, Injury Is Hard to Prove in Data-Breach Cases," The Wall Street Journal (June 26, 2016) (observing that injuries to consumers can be difficult to trace back to specific data breaches) (available at: https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988 (accessed Jan. 7, 2021)); *and* Edward T. Kang, "Data Breach Cases: An Analysis of Standing and Best Causes of Action," The Legal Intelligencer (Nov. 25, 2020) (identifying challenges with establishing standing after a data breach) (available at: https://www.law.com/thelegalintelligencer/2020/11/25/data-breach-cases-an-analysis-of-standing-and-best-causes-of-action/ (accessed Jan. 7, 2021)). *See also* Laura Caldera Taylor, Esq., and Thomas L. Hutchinson, Esq., "Identifying and Calculating Recoverable Damages and Predicting Risks in Cyber Security Breaches" (Summer 2014) (detailing some of the challenges with proving damages were proximately caused by particular data breaches) (available at: http://www.bullivant.com/files/Identifying-and-Calculating-

undertake activities that generate significant risk and, absent licensing, bonding, financial and insurance requirements, don't always have the financial means to take on the liability for the risks they are introducing, even if that liability could be pursued by the consumer or the data holder. Transparency also plays an important role here. Unless the consumer and data holder can clearly trace usage of the data, and there are mechanisms in place to alert consumers and data holders to breaches, it may be impossible to link a particular data aggregator's or data user's actions to a particular result that produces harm. An appropriate regulatory framework would need to address these issues along with supervision and enforcement of data aggregators and data holders in order to ensure that consumers and the financial ecosystem are appropriately protected.

Finally, TCH recommends that the Bureau undertake some study and evaluation of the requirements set forth in Regulation E, which predate the substantial changes that have taken place in the marketplace and that have been facilitated by data aggregation and other activities. As the Bureau's principles recognize, data aggregation activities are increasingly being leveraged to enable payment initiation. Those services frequently exist outside of the control of FI data holders and yet liability for unauthorized transfers and the costs of recredentialing continue to rest with them. It may be time to examine other constructs that could more fully align liability with responsibility and thereby provide appropriate incentives for all parties to safeguard consumer data.[77]

V. Conclusion

TCH and its member banks fully support the ability of consumers upon request to safely and securely obtain information about their ownership or use of a financial product or service from their product or service provider and have engaged in significant work with other industry stakeholders to facilitate that ability. Under the Principles developed by the Bureau, much progress has been made to further enable Consumers to do so in a safer, more secure, and more transparent way.

TCH recognizes, however, that more work remains and that market forces alone may not in some areas be sufficient to fully implement the Bureau's vision as outlined in the Principles. At the same time, a rulemaking by the Bureau is likely to be complex, time-consuming, and require the substantial commitment of both short-term and long-term resources in order to be successful. It will also need to envision the state of a rapidly developing market several years into the future – the approximate time it would take to promulgate a rule and have the rule become effective. Such an undertaking may also pose substantial risks to further industry progress if the industry were required to await key decisions from the Bureau on the path forward. Whatever action the Bureau takes, it will be

---

Recoverable-Damages-and-Predicting-Risks-in-Cyber-Security-Breaches.pdf (accessed Jan. 7, 2021); *and* David Cox and Gregory Jacobs, "Shouldn't Cyber-Insurance Cover Negligence?" ABA Insurance Coverage Litigation Committee Newsletter (Summer 2015) (detailing challenges associated with applying cause doctrines to data-breach-related damage determinations) (available at: https://www.kilpatricktownsend.com/~/media/Files/articles/2015/Shouldnt%20Cyber-Insurance%20Cover%20Negligence.ashx (accessed Jan. 7, 2021)).

[77] For example, one option might be for the Bureau to consider a system of warranties that would provide an appropriate legal basis for claims by consumers and data holders for damages caused by data aggregators and data users. A robust regulatory framework, however, would still be needed to ensure that data aggregators and data users had the financial wherewithal commensurate with the risks they introduced in order to meet any potential warranty claims.

important to align that action with the Principles, which have been the basis for so much industry progress, and to ensure that federal financial regulators are aligned and speaking with one voice.

If the Bureau does engage in a rulemaking, then it must do so in a holistic manner, addressing, at a minimum, the issues set forth above. The Bureau has been incredibly thoughtful in its work on this issue to date and TCH looks forward to continuing to engage with the Bureau as it works to determine the best path forward.

Respectfully submitted,

/S/

Robert C. Hunter
Deputy General Counsel & Director of Regulatory and Legislative Affairs

Appendix I – Analysis of Data Aggregator and Data User Terms and Conditions

Intuit	
Nature of Service	Unclear as there are potentially 5 different policies that need to be accessed and reviewed by the consumer, including (1) General Terms of Service, (2) Intuit Privacy Statement, (3) "Additional Terms and Conditions for the Services you have selected," (4) Third Party Privacy Statements "for the Services selected" and (5) "any terms provided separately to you for the Services…."
Data Accessed	Unclear as there are potentially 5 different policies that need to be accessed and reviewed by the consumer, including (1) General Terms of Service, (2) Intuit Privacy Statement, (3) "Additional Terms and Conditions for the Services you have selected," (4) Third Party Privacy Statements "for the Services selected" and (5) "any terms provided separately to you for the Services…."
Use	General Terms and Conditions give Intuit right to "maintain data" as part of the Services, and aggregate and use non-personally identifiable data. While an example is given of ways in which aggregated data may be used it is not exclusive and use is not otherwise specified. User Content may otherwise be used to provide "Services." More detail may be given in other documents.
Frequency	Unclear in General Terms and Conditions. May be addressed in other documents.
Retention Period	Unclear in General Terms and Conditions. May be addressed in other documents.
Liability Disclaimer	Use of the Services is "entirely at your own risk." Liability is "limited to the amount you paid for the Services during the 12 months prior to such claim." Indirect, special, incidental, punitive and consequential damages are specifically disclaimed as are damages from any "loss or theft of data."
User Termination	Unclear. Termination by consumers is unclear, but may include deletion (with deletion rights appearing to differ based on the state of residence). CA residents (and possibly users from other states, as deletion is mentioned generally in the "Information retention" section), "may have the right, under certain circumstances, to request that [Intuit] delete the personal information [consumers] have provided to [Intuit]." Unless deletion is specifically requested, Intuit "retain[s] your personal information as long as it is necessary to comply with our data retention requirements and provide [users] with services and the benefits of the Intuit Platform."

MX	
Nature of Service	Digital money management application that allows registered users to organize, consolidate, manage and track their financial information.
Data Accessed	Agreement lists third party provider account access numbers, passwords, security questions and answers, account numbers, login information, and "any other security or access information", and "the actual data in your user account(s) with such provider(s)" such as bank and other account balances, credit card charges, debits and deposits "as may be applicable."
Use	Account data may be used "to provide the services" Anonymous, aggregate data that does not contain PII may be used "for various purposes." Also references a separate Privacy Policy that user needs to consult. Privacy policy states that "we process data to fulfill our contractual obligations in our service contracts with clients and assist clients in optimizing advanced data analytics." Also notes that data may be used "to operate the business" and "to comply with applicable laws."
Frequency	"[T]he Services may 'refresh' the Provider Account Data by collecting the Provider Account Data nightly."
Retention Period	Unclear. Users grant MX the right to use account data "without any particular time limit."
Liability Disclaimer	"MX specifically disclaim (sic.) any liability, loss, or risk which is incurred as consequence, directly or indirectly, of the use and application of any of the content on this site." The disclaimer includes "[a]ny loss resulting from, including any unauthorized access by a third party, arising out of or related to your access and/or use of or interaction with the Services or the Materials." MX specifically disclaims any warranties that the site or services will be secure. Limitation on liability provides that MX "shall not be liable" for compensatory, incidental, indirect, direct, special, punitive, consequential, or exemplary damages "however caused" including specifically damages related to loss, security or theft of data and "loss of privacy."
User Termination	MX retains (and may use) the personal data of its clients' customers "for a period of time as instructed by the clients for whom MX processes data…." To request deletion of data, consumers must "contact directly the client who provided the source of data." Where "MX collects personal data for its own purposes, it retains the data for a reasonable period of time to fulfill the processing purposes [noted in the terms]." The terms note that certain U.S. individuals and households may have personal data rights, including the right to request deletion of personal information, under the CCPA.

Plaid	
Nature of Service	Unclear. Will depend on end-user application.
Data Accessed	Unclear. Will depend on end-user application. Plaid's End User Privacy Policy, however, notes that it collects "identifiers and login information required by the provider of your account, such as your username and password, or a security token. In some cases, we also collect your phone number, email address, security questions and answers, and one-time password (OTP)…." Further, while the Privacy Policy gives examples of various types of information Plaid may obtain, Plaid notes that "The information we receive from the financial product and service providers that maintain your financial accounts varies depending on the specific Plaid services developers use to power their applications, as well as the information made available by those providers."
Use	Unclear. Will depend on end-user application. Plaid's End User Privacy Policy notes that "[w]e use your End User Information for a number of business and commercial purposes, including to operate, improve, and protect the services we provide, and to develop new services" and gives a number of examples of how data may be used, including "to operate, provide and maintain our services."
Frequency	Unclear and not addressed by the End User Privacy Policy. May depend on end-user application.
Retention Period	Unclear. Plaid's End User Privacy Policy states that Plaid retains "End User Information for no longer than necessary to fulfill the purposes for which it was collected and used, as described in this Policy*, unless a longer retention period is* required or *permitted under applicable law*" (emphasis added). The Policy goes on to state, "[a]s permitted under applicable law, even after you stop using an application or terminate your account with one or more developer, we may still retain your information." While the policy gives an example of an end-user retaining an account with another Plaid developer, that example would not appear to be exclusive.
Liability Disclaimer	Not addressed directly. Plaid's Developer Policy, however, states that "Plaid will not be liable for any damages of any nature suffered by you or any third party resulting from Plaid's exercise of its rights under this policy or under applicable law."
User Termination	Unclear. Retained data may be used by Plaid, subject to requests for deletion of End User Information contained in the "Your Data Protection Rights" section, which provides CA residents with the right to request deletion of their personal information pursuant to the California Consumer Privacy Act. Separately, accounts may be deactivated, but it is unclear what End User Information remains post-deactivation (Plaid states that "[o]nce you stop using the Service in accordance with any applicable agreement you may have with us, you may deactivate your Account by following the instructions on the Site," and that after deactivation Plaid will "deprovision your access to all End User Data associated with your integration," but that "Plaid may still retain any information [it] collected about you for as long as necessary to fulfill the purposes outlined in [its] privacy policy/statement, or longer retention period if required or permitted under applicable law."

Yodlee (Envestnet / Yodlee)	
Nature of Service	Unclear. Will depend on end-user (Yodlee Service) application.
Data Accessed	Unclear. Will depend on end-user (Yodlee Service) application. Yodlee's Privacy Notice states that "[i] n order to display information to you through the Yodlee Services, the Services must collect, on your behalf, your account and other personal information from third party web sites and Internet services that you register on the Yodlee Services."
Use	Unclear. Will depend on end-user (Yodlee Service) application. Yodlee's Privacy Notice provides that information will "not be sold, shared, rented or traded with any affiliated or unaffiliated third parties, *except (i) to provide you with the Yodlee Services , (ii) pursuant to joint marketing arrangements described below, or (iii) as required or permitted by law*" (emphasis added). Further, Yodlee's Privacy Notice states that "in order to provide you with the Yodlee Services, Yodlee may disclose your username and passwords to third party web sites, such as web sites operated by a credit card company or a bank, in order to obtain the information that you requested be aggregated and displayed through the Yodlee Services" and that unless certain opt-outs apply, Yodlee may "disclose registration information and information on your use of the Yodlee Services (excluding information regarding transactions on your aggregated accounts) to companies that perform marketing services on our behalf, or to other financial institutions with whom Yodlee offers you products and services pursuant to joint marketing agreements."
Frequency	Unclear and not addressed by the Yodlee Privacy Notice. May depend on end-user (Yodlee Service) application.
Retention Period	Unclear. Yodlee's Privacy Notice states that Yodlee "will collect and retain your personal information, both the information you provide directly and the information we obtain from third party sites, for as long as actively required for you to use the data in the Yodlee Services," and that after cancellation of a Yodlee Service it "reserve[s] the right to retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements." If a consumer cancels his Yodlee Service, then the Yodlee Privacy Notice states that Yodlee "will discontinue the collection of information from third party sites on your behalf."
Liability Disclaimer	Not addressed directly. Since Yodlee has no direct contractual or other relationship with the end-user consumer (the policies and terms and conditions of the Yodlee Service provider apply). Yodlee's Developer Terms, however, state that "to the maximum extent permitted by law, [the developer] agrees that neither Yodlee nor any of its affiliates, subsidiaries, licensors, suppliers, third party developers, data sources or any of their affiliates (collectively, 'Yodlee Parties') will be liable for any direct, indirect, punitive, incidental, special, consequential or exemplary damages arising out of or relating to the services or this agreement, including, but not limited to, damages for loss of profits, opportunity, goodwill, use, data or other intangible losses" (capitalization removed).
User Termination	Unclear. Retained data may be used by Yodlee, with Yodlee's clients' "data governance and privacy practices applicable to those services." It is unclear how consumers terminate,

	although the Yodlee Privacy Notices states that someone no longer desiring Yodlee's services may delete their personal information in their personal profile form or by submitting a service request. CA residents may request deletion of their personal information pursuant to the California Consumer Privacy Act and Yodlee's Privacy Notice for CA Residents.

Acorns	
Nature of Service	A subscription-based service that offers investment advice, investment services, and, through partnerships with banks, demand deposit and other banking products and services, including transactional and payment services.
Data Accessed	Acorns' Master Privacy Policy notes that Acorns collects "contact information such as name, email address, mailing address, phone number; billing information such as credit card number, and billing address; financial information such as bank or brokerage account numbers, types of investments; Social Security number; driver's license number; unique identifiers such as username, account number, password; preferences information such as product wish lists, order history, and marketing preferences; and demographic information such as age, education, gender, interests, and zip code." In addition, the Master Privacy Policy notes that Acorns collects personal-device-related information, such as the type of device you use, operating system, the device identifier (or "UDID"), your IP address, location, mobile network information, and standard web log information, such as your browser type traffic to and from our site, the pages you accessed on our website, and other available information" and information based on usage history, such as details of purchases, "content you viewed, event information, click stream information, and cookies that may uniquely identify your browser or your account."
Use	Unclear. Information use is governed by the Master Privacy Policy, potentially by other companies' privacy policies (e.g., Plaid), or other Acorns agreements/terms, and use of certain Acorns products and services (e.g., activation/use of the Acorns debit card). Under the Master Privacy Policy, Acorns uses and discloses personal information "to analyze site usage and improve the Service; to deliver to you any administrative notices, money alerts, and communications relevant to your use of the Service; to fulfill your requests for certain products and services; for market research, project planning, troubleshooting problems, and detecting and protecting against error, fraud, or other criminal activity; to third-party contractors that provide services to Acorns and are bound by these same privacy restrictions; to enforce Acorns' Terms of Use; and as otherwise set forth in this Privacy Policy," which includes "connecting [users] with people [they] already know," sharing with Plaid as a service provider (which permits personal and financial information to be "transferred, stored, and processed by Plaid in accordance with Plaid's end user privacy policy," and additional use of personal and financial information (including transaction information) for activation and use of Acorns payment products and programs (e.g., the Acorns debit card and Local Found Money program).
Frequency	Unclear in the Acorns Master Privacy Policy, Important Disclosures, or Terms of Use. May be addressed in other documents, such as agreements for specific products or services.
Retention Period	The Acorns Master Privacy Policy provides for Acorns to "retain and use … information as necessary to comply with [Acorns'] legal and/or regulatory obligations, resolve disputes, and enforce [Acorns'] agreements." Information retention is not addressed in the Acorns Important Disclosures or Terms of Use.

Liability Disclaimer	Acorns' Important Disclosures provide that "[i]n no event shall Acorns, its respective affiliates, directors, officers, registered representatives, or employees, be liable for any damages of any kind (including, without limitation, special, incidental, indirect, or consequential damages) on any theory of liability arising out of or in connection with the use of any information on this website" (it is unclear whether this is meant to disclaim liability for all Acorns' products and services; however, the Important Disclosures state separately that "Acorns is solely responsible for the application and website content," suggesting that this is meant to be comprehensive, and Acorns' Terms of Use contain lengthy, additional disclaimers. Acorns' Terms of Use also provide that use of Acorns' services is at one's own risk, stating that "[a]ny use or reliance on any Content or Materials of other users posted via the Services or obtained by you through the Services is at your own risk" and that Acorns does not "endorse, support, represent or guarantee the completeness, truthfulness, accuracy, or reliability of any Content or Materials posted via the Services or endorse any opinions expressed via the Services."
User Termination	Unclear. Terminating service by making changes on the customer information page, or by emailing Acorns Customer Service, does not appear to necessarily terminate information use or disclosure by Acorns. Similarly, it is unclear whether a customer exercising his termination rights pursuant to Sections 7, 8.3, 8.4, or 8.5 of the Acorns Program Agreement also terminates information use or disclosure by Acorns. CA residents may request deletion of their personal information pursuant to the California Consumer Privacy Act by emailing support@acorns.com.

LendingClub	
Nature of Service	LendingClub facilitates "peer-to-peer" lending by matching borrowers and lenders (including personal and business loans). LendingClub also provides financial education.
Data Accessed	LendingClub's Privacy Policy states that LendingClub "collect[s] information you provide LendingClub when you interact with us directly or through a third-party, such as when you register for our Service, apply for a loan or to be an investor, sign up for our mailing list, or otherwise communicate with us." The precise information gathered depends on the interaction with LendingClub, but broad-based gathering is provided for, with myriad categories of personal information able to be collected and used under the Privacy Policy. This includes: (i) Identifying Information (such as "a real name, alias, postal address, telephone number, unique personal identifier, online identifier, Internet Protocol address, email address or other communication information, account name, social security number, driver's license number or state identification card number, passport number, or other similar identifiers or identity verification information" as well as club membership or reward-based program identifiers"); (ii) Financial Information (such as "payment and bank information, wire transfer information, credit card number, debit card number, full credit report, transactional information for financial accounts, account information including interest rates and balances, income information, and any other financial information available"; (iii) Commercial Information (such as "records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies"); (iv) Business Information (such as "legal business name and company practice name, and other information about your company or practice such as fax, telephone number, website, relevant email addresses, physical address, business related licensing information such as a license number, federal tax identification or social security number, and business or practice bank account information"); (v) Network Activity and Location Information (such as "your browsing history, search history, geolocation data, and information regarding your interaction with an Internet

	web site, application, or advertisement"); (vi) Audio, Visual, and Electronic Information (such as "a picture of you, digital or digitized signature, or voice recordings from phone calls" and "communications between you and LendingClub"); (vii) Professional, Education, or Employment-related Information (such as "work history, employer and employment information, profession, job title, work address and phone number, and other information related to your profession"; (viii) Other Sensitive Information (such as "your transactions with us or provided to us through linked accounts and systems, such as information about medical or educational services purchased with a loan, [or] insurance information"); and (ix) Inference Information (inferences drawn from any other information gathered).
Use	Information use and sharing under the Privacy Policy depends on interaction/application, and the specific type of information gathered, but is similarly broad-based and is largely used for LendingClub to improve and expand its own services. In addition, LendingClub works with other companies, such as Plaid, to obtain information. In such instances, information shared with the third party incorporates that third party's privacy policies/terms and conditions (the LendingClub Privacy Policy notes that when financial information is provided to a third party, "such information accessed, collected, or transmitted by the third party for this purpose will be governed by the privacy policy of the third party." In general, LendingClub's Privacy Policy provides for use as follows: (i) Identifying information is used "to verify your identity, facilitate transactions, to advertise to you, and to create your borrower or investor profile and account;" to "invite your friends and contacts to connect with our Service and to provide credit to you for referrals," and to communicate; (ii) Financial Information is used "to process your transaction, to improve and expand our Service, and to determine your financial health;" (iii) Commercial Information is used to determine creditworthiness and financial health, to improve and expand LendingClub's Service and protect its security interests; (iv) Business Information is used to process applications, facilitate transaction, for verification purposes, and to improved and expand LendingClub Services; (v) Network Activity and Location Information is used for "security, processing your application, facilitating transactions, marketing, for verification purposes and to improve or expand [LendingClub's] Services;" (vi) Audio, Visual, and Electronic Information is used "for information security, fraud detection and prevention, quality control, and for processing your application, facilitating transactions, for verification purposes and to improve or expand [LendingClub's] Services;" (vii) Professional, Education, or Employment-related Information is used "to determine [ ] creditworthiness if you are a borrower, assess risks related to your potential loan, and to help investors determine whether to commit to or purchase your loan," as well as to enable or implement automatic payments, improve and expand LendingClub's Services, for verification services, or for product offerings; (viii) Other Sensitive Information is used to "process [ ] loan applications, facilitat[e] transactions, for verification purposes, regulatory requirements, to improve or expand [LendingClub's] Services, and to offer products and Services…;" and (ix) Inference Information is used for marketing or to improve or expand LendingClub's Services. The LendingClub Privacy Policy also provides for information sharing for myriad reasons (*see* §§ 1, 3 and 5), and notes that LendingClub does not sell personal information as defined in the California Consumer Protection Act.
Frequency	The LendingClub Privacy Policy does not specify the frequency with which personal information is gathered. Certain information would ostensibly be gathered as part of a specific application process or other single process, but other information could be gathered or obtained for a variety of reasons, possibly subject to separate product or service agreements.
Retention Period	The LendingClub Privacy Policy and Terms of Use do not specify a data retention period. However, the Privacy Policy states that LendingClub "may not be able to modify or delete information in all circumstances;" that "[d]ue to the regulated nature of [LendingClub's] industry, [it] [is] under legal requirements to retain data and [is] generally not able to delete

	consumer transactional data upon request;" that "[c]ertain regulations issued by state and/or federal government agencies may require [LendingClub] to maintain and report demographic information on the collective activities of [its] membership;" and that LendingClub "may also be required to maintain information about you for at least seven years to be in compliance with applicable federal and state laws regarding recordkeeping, reporting, and audits." And the Terms of Use provide for User Content provided to LendingClub (including personal information provided) to be subject to a perpetual, irrevocable license (the Terms of Use state that "[b]y posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing."
Liability Disclaimer	The Lending Club Borrower Agreement, which "governs the process by which you may make a request or requests for a loan from us through the website LendingClub.com, including any subdomains thereof, or other applicable channels offered by us…" contains a broad disclaimer of liability, stating that: "IN NO EVENT SHALL WE BE LIABLE TO YOU FOR ANY LOST PROFITS OR SPECIAL, EXEMPLARY, CONSEQUENTIAL OR PUNITIVE DAMAGES, EVEN IF INFOMRED OF THE POSSIBILITY OF SUCH DAMAGES."
User Termination	Unclear. The Privacy Policy notes that LendingClub "may not be able to modify or delete information in all circumstances;" and that California residents possess the right to request LendingClub delete certain personal information that LendingClub has collected from the consumer, pursuant to the California Consumer Privacy Act (CCPA) (but that "[m]ost of the information [LendingClub] collect[s] is subject to [the Gramm-Leach-Bliley-Act] and [is] therefore not subject to the CCPA). Further, the Terms of Use provide that LendingClub's license to use User Content does "not expire" when users remove User Content from the Site (users may remove their User Content from the Site at any time). LendingClub's Consumer Privacy Notice provides for an opt-out of sharing with certain affiliates and nonaffiliates, pursuant to the Gramm-Leach-Bliley-Act.

Robinhood	
Nature of Service	Robinhood provides brokerage and investment advisory services, as a registered broker-dealer; in addition, Robinhood, through partnerships with banks, offers a debit card program and other financial products and services.
Data Accessed	The precise information gathered depends on the interaction with Robinhood, and the service or account requested, but broad-based gathering is provided for under Robinhood's United States Privacy Policy (Privacy Policy). For example, the Privacy Policy notes that Robinhood collects: (i) Identity Data (including "full name, date of birth, gender, social security numbers, and other data on government-issued identification documents"); (ii) Contact Data (email, mailing address, and telephone); (iii) Financial Data (including "bank account and payment card details, suitability information, and information about your income, account balances, financial transaction history, credit history, tax information, and credit scores"); (iv) Profile Data (including "bank account and payment card details, suitability information, and information

	about your income, account balances, financial transaction history, credit history, tax information, and credit scores"); (v) Usage Information (including information about access and use of Robinhood Services, such as user actions on the Services, including interactions with others on the Services, uploaded photos or media, usernames, and other content provided by users); (vi) Contact List Information, with permission; and (vii) Additional Information (including information submitted via focus groups, contests/sweepstakes, job applications, customer support, or other similar means). In addition, the Privacy Policy notes that location data, usage data, and personal device data are gathered through tracking technologies, and that information about persons is obtained from third parties.
Use	The Privacy Policy notes that information, including personal information, may be used as described, or as otherwise described on or in connection with Robinhood Services, including to: (a) "Create and process your account and deliver the Services to you, including to allow you to register for the Services and participate in interactive features and for Robinhood to authenticate your identity, handle billing and account management, fulfill our legal and regulatory obligations such as obligations that apply to being a regulated broker-dealer, and complete other administrative matters;" (b) "Send [ ] transactional information, including confirmations, invoices, technical notices, product and services information and announcements, software updates, security alerts, support and administrative messages, and information about [ ] transactions with us;" (c) for communications (e.g., to respond to comments and questions, deliver newsletters or other content, to provide customer service or feedback, or for any other purposes in connection with the Services); (d) to "[c]onduct research and analytics to understand [Robinhood's] visitors and customers and tailor [its] product offerings;" (e) to provide updates about products and services Robinhood and its partners offer; (f) to make product and service suggestions and recommendations to users; (g) to "[m]onitor, administer, and enhance [Robinhood's] Services;" (h) to "[e]nhance the safety and security of [Robinhood's] Services, business, and users, and investigate or provide notice of fraud or unlawful or criminal activity;" and (i) for legal purposes (to perform audits, protect or exercise legal rights, carry out contracts and agreements, and demonstrate compliance with applicable laws and legal obligations). In addition, the Privacy Policy notes that personal information may be shared with authorized third-party vendors and service providers, with companies with which Robinhood users hold securities, with Robinhood affiliates, for substantial corporate transactions, for legal purposes, and with consent.
Frequency	Unclear in the Privacy Policy, Robinhood Financial LLC & Robinhood Securities, LLC Customer Agreement, and select product agreements (e.g., Robinhood Debit Card Agreement). May be addressed in other documents.
Retention Period	Unclear in the Privacy Policy, Robinhood Financial LLC & Robinhood Securities, LLC Customer Agreement, and select product agreements (e.g., Robinhood Debit Card Agreement). May be addressed in other documents.
Liability Disclaimer	The Robinhood Financial LLC & Robinhood Securities, LLC Customer Agreement provides a broad disclaimer and liability limitation. It states, in part, that ". EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS AGREEMENT, I UNDERSTAND AND AGREE THAT ROBINHOOD, ITS AFFILIATES, THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES AND AGENTS, AND THE PROVIDERS (COLLECTIVELY THE 'ROBINHOOD PARTIES') WILL NOT BE LIABLE TO ME OR TO THIRD PARTIES UNDER ANY CIRCUMSTANCES, OR HAVE ANY RESPONSIBILITY WHATSOEVER, FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING TRADING LOSSES, DAMAGES, LOSS OF PROFITS, REVENUE, OR GOODWILL) THAT I MAY INCUR IN CONNECTION WITH MY USE OF THE SERVICE PROVIDED BY ROBINHOOD OR ANY OF ITS AFFILIATES UNDER THIS AGREEMENT (INCLUDING MY USE OF THE APP, THE

	WEBSITE, THE MARKET DATA, THE INFORMATION, OR THE CONTENT), BREACH OF THIS AGREEMENT, OR ANY TERMINATION OF THIS AGREEMENT, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT FORESEEABLE, EVEN IF ANY ROBINHOOD PARTY HAS BEEN ADVISED OR WAS AWARE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. THE ROBINHOOD PARTIES SHALL NOT BE LIABLE BY REASON OF DELAYS OR INTERRUPTIONS OF THE SERVICE OR TRANSMISSIONS, OR FAILURES OF PERFORMANCE OF THEIR RESPECTIVE SYSTEMS, REGARDLESS OF CAUSE, INCLUDING THOSE CAUSED BY GOVERNMENTAL OR REGULATORY ACTION, THE ACTION OF ANY EXCHANGE OR OTHER SELF REGULATORY ORGANIZATION, OR THOSE CAUSED BY SOFTWARE OR HARDWARE MALFUNCTIONS." It further provides that "[e]xcept as otherwise provided by law, Robinhood or any of its affiliates or respective partners, officers, directors, employees or agents (collectively, "Indemnified Parties") shall not be liable for any expenses, losses, costs, damages, liabilities, demands, debts, obligations, penalties, charges, claims, causes of action, penalties, fines and taxes of any kind or nature (including legal expenses and attorneys' fees) (whether known or unknown, absolute or contingent, liquidated or unliquidated, direct or indirect, due or to become due, accrued or not accrued, asserted or unasserted, related or not related to a third party claim, or otherwise) (collectively, "Losses") by or with respect to any matters pertaining to My Account, except to the extent that such Losses are actual Losses and are determined by a court of competent jurisdiction or an arbitration panel in a final non-appealable judgment or order to have resulted solely from Robinhood's or any of its affiliates' gross negligence or intentional misconduct."
User Termination	Unclear. The Privacy Policy notes that the California Consumer Privacy Act "provides California residents the right to request more details about the categories and specific elements of personal information we collect, to delete their personal information, to opt out of any 'sales' that may be occurring, and to not be discriminated against for exercising these rights," but states that Robinhood does not sell information to third parties. Robinhood's Consumer Privacy Notice provides for an opt-out of sharing with certain affiliates, pursuant to the Gramm-Leach-Bliley-Act.

Venmo	
Nature of Service	Venmo is a payment service provider (a licensed provider of money transfer services).
Data Accessed	The Venmo Privacy Policy notes that Venmo collects information when an account is opened, including (i) Account Information (including text-enabled cellular/wireless telephone number, machine or mobile device ID and other similar information); (ii) Identification Information (including your name, street address, email address, date of birth, and SSN (or other governmental issued verification numbers)); (iii) Device Information (information from mobile devices and computers, and other sources); (iv) Geolocation Information (including information that identifies with reasonable specificity your location by using, for instance, longitude and latitude coordinates obtained through GPS, Wi-Fi, or cell site triangulation); (v) Social Web Information (including Facebook Connect credentials and email account information, and, if authorized, email addresses, Facebook friends lists, and public profiles); and (vi) Financial Information (including bank account online login information, bank account and routing numbers and credit cards linked to your Venmo account). In addition, the Privacy Policy notes that Venmo "may also obtain information about you from third parties such as identity verification, fraud prevention and similar services" and "may collect additional information from or about you in other ways not specifically described [in the Privacy Policy]." The Privacy Policy also provides that aggregated and/or anonymized data is not considered personal information if it does not identify a specific user.
Use	The Venmo Privacy Policy provides for use of personal information for the following purposes: (a) to "provide the services and customer support you request;" (b) to "process transactions and send notices about your transactions or your network activity;" (c) to "resolve disputes, collect fees, and troubleshoot problems;" (d) to "prevent potentially fraudulent, prohibited or illegal activities, and enforce our User Agreement through the use of our risk and fraud tools which may include use of Account Information, Identification Information, Financial Information, Device Information, Social Web Information and Geolocation Information;" (e) to "create an account connection between your Venmo account and a third-party account or platform;" (f) to "customize, personalize, measure, and improve our services and the content and layout of our website;" (g) to "send you updates about new products and services that we are offering to customers;" (h) to "compare information for accuracy and verify it with third parties; perform other duties as required by law;" and (i) "if you elect to share your Geolocation Information, we will use this information to enhance the security of the Services and we may use this information to provide you with location-specific options, functionality, offers, advertising, search results, or other location-specific content." Further, the Privacy Policy provides for the sharing of personal information for specific, payment-related purposes (noting that personal information will be shared with persons or companies that a user is paying or that are paying a user, in order to process payments on Venmo; and that "contact information, date of sign-up, the number of payments you have received and other verification metrics like social graph activity may be provided to users or companies when you transact with, on, or through Venmo"), and notes that "[s]ome personal information is public information," including Venmo usernames, profile photos, first and last names, the month and year of Venmo account creations, and public transactions." Any logged-in Venmo user may also see any other Venmo user's friends list.
Frequency	Unclear in the Privacy Policy and User Agreement. May be addressed in other documents.

Retention Period	Unclear in the Privacy Policy and User Agreement. May be addressed in other documents.
Liability Disclaimer	The User Agreement provides for indemnification of PayPal and limitation of liability, stating, in part, that "[y] ou agree to defend, indemnify and hold PayPal harmless from any claim or demand (including reasonable legal fees) made or incurred by any third party due to or arising out of your breach of this user agreement, your improper use of the Venmo services, your violation of any law or the rights of a third party and/or the actions or inactions of any third party to whom you grant permissions to use your Venmo account or access our websites, software, systems (including any networks and servers used to provide any of the Venmo services) operated by us or on our behalf, or any of the Venmo services on your behalf" and that "[i] n no event shall PayPal be liable for lost profits or any special, incidental or consequential damages (including without limitation damages for loss of data or loss of business) arising out of or in connection with our websites, software, systems (including any networks and servers used to provide any of the Venmo services) operated by us or on our behalf, any of the Venmo services, or this user agreement (however arising, including negligence), unless and to the extent prohibited by law."
User Termination	Unclear. The User Agreement generally provides that users may close their accounts and terminate their relationship without cost. However, the Privacy Policy notes that "[w]hen you are no longer our customer, [Venmo] continue[s] to share your information as described in this policy." The Privacy Notice observes that California residents have the right to request deletion of personal information under the California Consumer Privacy Act, notes that Venmo collects, uses, and shares personal information regarding California residents as described in the Privacy Notice, and provides a hyperlink and phone number for California residents to contact Venmo.