The Clearing House

January 25, 2023

Via email to Financial_Data_Rights_SBREFA@cfpb.gov

Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Comments on Small Business Review Panel for Required Rulemaking on Personal Financial Data Rights—Outline of Proposals and Alternatives Under Consideration

Ladies and Gentlemen:

The Clearing House Association L.L.C. ("TCH")[1] appreciates the opportunity to comment on the outline of proposals under consideration by the Consumer Financial Protection Bureau ("CFPB" or "Bureau") for its rulemaking on personal financial data rights under section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act").[2] While TCH's members are large financial institutions that are not small businesses as defined in the Small Business Regulatory Enforcement Fairness Act of 1996 ("SBREFA"),[3] they each have considerable experience facilitating data access and appreciate the Bureau's willingness to extend the SBREFA consultative process to include comments from stakeholders beyond the small business community.

TCH and its member banks fully support the right of consumers to safely and securely obtain information, upon request, about their ownership or use of a financial product or service from the provider of that product or service. As more fully detailed in this letter, TCH and its members have engaged in significant work with other industry stakeholders to facilitate that right. That work, which has involved the commitment of substantial time, effort, and resources, has been undertaken in conformance with the principles for consumer-authorized financial data sharing and aggregation that the Bureau released in October 2017 ("Principles").[4] The Bureau has neither retracted nor amended the Principles since their original publication, and they remain on the Bureau's website. As the Bureau moves forward with its rulemaking on personal financial data rights, it is important that the rulemaking be guided by the Principles to ensure that the final rule is minimally disruptive of and does not diminish the substantial progress that has already been made

[1] TCH, the country's oldest banking trade association, is a nonpartisan organization that provides informed advocacy and thought leadership on critical payments-related issues. Its sister company, The Clearing House Payments Company L.L.C. ("TCH PayCo"), owns and operates core payments system infrastructure in the United States, clearing and settling more than $2 trillion each day. See The Clearing House's website at www.theclearinghouse.org.

[2] Pub. L. No. 111-203, § 1033, 124 Stat. 1376, 2008 (codified at 12 U.S.C. § 5533).

[3] Pub. L. No. 104-121, tit. II, 110 Stat. 847, 857–74 (1996) (codified at 5 U.S.C. §§ 601–11 as amended by Dodd-Frank Act § 1100G).

[4] CFPB, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017) (hereinafter "Principles").

by the private sector in creating an infrastructure that facilitates safe, secure data sharing consistent with the Bureau's previously issued guidance.

TCH recognizes that this SBREFA consultation is "only one step in the CFPB's rulemaking process" and that many of the proposals and alternatives the Bureau discusses in its outline ("SBREFA Outline") will need further refinement and definition as the rulemaking process moves forward.[5] TCH looks forward to further dialogue with the CFPB as the rulemaking process unfolds. In part I of this letter, TCH summarizes its observations and recommendations, which are more fully analyzed in the body of this letter and which it hopes will be helpful as the CFPB continues to iterate toward a final rule. Part II of this letter discusses the foundational work in this area the Bureau already did—namely, the Principles it issued in 2017. Part III describes a series of initiatives undertaken by the private sector in the wake of the Principles to promote and facilitate consumers' personal financial data rights. Parts IV through XII lay out in more detail our recommendations and observations in response to individual questions the Bureau raised in the SBREFA Outline.

I. Summary of Observations and Recommendations

General Observations and Recommendations

- The industry has already done substantial work to provide safe, secure consumer-authorized data sharing to over 42 million U.S. consumers. It is imperative that any further action taken by the Bureau be consistent with its prior positions articulated in the Principles and be coordinated with other federal financial services regulators to ensure that the industry's accomplishments are not diminished and that a consistent approach to issues relating to consumer-permissioned data access is maintained.
- Industry stakeholders across the data-sharing spectrum have, through FDX, done substantial work to create data-sharing standards that work well, are broadly used in the market today, and are consistent with the well-considered and longstanding Principles. The Bureau should ensure that any final rule allows for the continued use of those standards.
- To ensure meaningful compliance with any section 1033 rule, the Bureau must ensure, through a larger participant rulemaking or other assertion of supervisory authority, that third parties are subject to appropriate supervision and enforcement based on the risks they pose to consumers.
- Credential-based access and screen scraping have inherent risks and are inevitably harmful to consumers; both practices should be sunsetted. The industry should be transitioned to a safer, more secure application programming interface ("API") environment that allows for greater consumer transparency and control. The ban on screen scraping should go beyond the narrow definition of "covered accounts" and encompass the practice in its entirety. Credential-based access and screen scraping should not be allowed in any circumstance once a covered data provider has provided API access. Further, once API access is made available, third parties should be required to delete all information associated with or gained through screen scraping, including customer credentials.

[5] *See* CFPB, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights: Outline of Proposals and Alternatives Under Consideration 7 (Oct. 27, 2022) (hereinafter "SBREFA Outline").

Related Statutes and Regulations

- The Bureau has indicated that it is considering incorporating into its rulemaking certain consumer rights regarding "inaccurate data." Depending on how the Bureau proceeds, these could conflict with consumer rights in the Electronic Fund Transfer Act ("EFTA") and Regulation E, the Truth in Lending Act ("TILA") and Regulation Z, the Truth in Savings Act ("TISA") and Regulation DD, and the Real Estate Settlement Procedures Act of 1974 ("RESPA") and Regulation X. TCH strongly believes that EFTA/Regulation E and TILA/Regulation Z should continue to exclusively govern the substantive rights of consumers and the obligations of financial institutions in connection with electronic fund transfers and credit cards and credit card accounts, respectively, as to what constitutes an error and responsibilities for error resolution. Similarly, TCH strongly believes that TISA/Regulation DD and RESPA/Regulation X should continue to exclusively govern the obligations of depository institutions and other covered entities to identify and correct inaccurate data within their purview.
- The Bureau has indicated that the provision of credit reports by data providers may be within the scope of its section 1033 rulemaking. To ensure the data is appropriately current and usable, TCH believes that consumers and authorized third parties should obtain credit reports directly from consumer reporting agencies. Depending on how the Bureau proceeds, the Fair Credit Reporting Act ("FCRA") and Regulation V may need to be amended to permit such information sharing. TCH strongly believes that FCRA/Regulation V should continue to exclusively govern consumer rights with respect to data accuracy and error resolution concerning data collected and reported by consumer reporting agencies. In addition, the extent to which FCRA would apply to permissioned data and what obligations, if any, would be imposed on various stakeholders need to be clarified; TCH submits that data providers cannot and should not be subject to FCRA requirements relating to furnishers of information.
- The requirements of the Gramm-Leach-Bliley Act ("GLBA") and Regulation P—and the potential liability imposed for violations thereunder—strongly suggest that authorization should take place at the data provider (and not at the third party, as the Bureau seems to envision) as authorization at the data provider is the only way the data provider would be reasonably assured that the consumer's authorization was valid and in accordance with the requirements of GLBA/Regulation P. In addition, the Bureau would likely need to amend Regulation P to ensure consistency of the authorization disclosures that would have to be provided by the covered financial institution under both the Bureau's section 1033 rule and Regulation P.
- The Office of the Comptroller of the Currency ("OCC") and other federal financial services regulatory agencies have issued detailed guidance on third-party risk management that their regulated financial institutions are expected to follow. The Bureau must make appropriate accommodations in any section 1033 rulemaking for prudential regulatory agency guidance on third-party risk management.

Coverage of Data Providers

- To comply with the statutory mandate in section 1033 and to achieve the more competitive marketplace the Bureau intends this rulemaking to foster, the scope of covered data providers must be enlarged from what was proposed in the SBREFA Outline. The limited scope of data providers covered by the Bureau's proposal would substantially diminish the extensive data-

sharing ecosystem that the private sector has already developed and would thereby harm consumers by actually decreasing their ability to share data. Furthermore, such a limited scope is inconsistent with the mandate under section 1033 itself to provide consumers broad access to information about the financial products and services they use from the providers of those products and services.

Recipients of Information

Direct Access by Consumers

- The Bureau notes that it is considering proposing that a covered data provider satisfy its obligation to make information directly available to a consumer by making the information available either to the consumer who requests the information or to all the consumers on a jointly held account. TCH appreciates the flexibility the Bureau's proposal suggests. Given that different types of accounts have varying account terms, legal requirements, and authorization requirements, banks will need flexibility in determining how best to meet customers' needs for the information they seek and the legal obligations which the banks themselves have.
- Given the important relationship that consumers have with their financial institutions, coupled with the inherent risks associated with sharing sensitive consumer data with unaffiliated third parties, the Bureau, as part of any rulemaking, should strongly encourage the direct transfer of data to the consumer.

Third-Party Access

- The Bureau notes that it is considering certain disclosure requirements. The Bureau should develop disclosure requirements for all parties that are consistent with Principle 3. Such requirements may also include model disclosures that create a safe harbor for users. Disclosure requirements should apply to both data providers and third parties. The obligation on data providers should generally be limited to disclosing to whom data is initially and directly provided, the fact that the provision of data was authorized, and identification of the appropriate mechanism to halt the provision of data. Third parties should be required to disclose the identity of each data user to whom the consumer's data is being provided, and each data user with which the information is shared should be required to obtain separate and distinct authorization from the consumer for use of the data. Disclosure by third parties should include what data is being accessed, how frequently and for what purpose it is being accessed, and for how long it is stored. Third-party disclosures should spell out the consumer's right to revoke authorization and should include the consumer's right to be forgotten. Disclosures regarding data use and how to revoke authorization should be provided on a standing basis, in addition to being provided immediately prior to authorization. Consumers should be required to affirmatively approve the specific data categories for which they wish to provide access.
- The Bureau should prohibit the sale of consumer data unrelated to the direct provision of any authorized product or service to the consumer.
- Data providers should have the right to build API services in a way that allows the consumer to control the flow of data and the scope of authorization at the data provider.

- To ensure consumers continue to wish to provide their data, data providers should have the right to set reasonable periodic reauthorization requirements that work for the data providers and their customers. In the event the Bureau does not provide for authorization at the data provider, it should establish a periodic reauthorization requirement of reasonably short duration, with reauthorization required more frequently after a period of nonuse (e.g., 90 days).
- The Bureau should address what rights and protections a consumer has if a data recipient, once in possession of the consumer's data, transfers that data outside the United States.
- The authorization process the Bureau seems to contemplate taking place at third parties is at odds with the goal of protecting consumers from fraud and other misuse and with how well-functioning authorization is usually accomplished in an API environment today. The Bureau should reimagine its authorization proposal to ensure it complies with existing standards.

Types of Information a Covered Data Provider Would Be Required to Make Available

- Data access in all instances should be limited by the particular use case at issue consistent with the principle of data minimization.
- Third parties should obtain only those types of data they need for the product or service then being provided regardless of use case. Consumers should be fully in control of which categories of data are being provided, to whom, for how long, and for what purpose, regardless of use case.

Periodic Statement Information for Settled Transactions and Deposits

- To control and lower instances of fraud, data providers should have the option of sharing tokenized account numbers and routing numbers with authorized third parties in lieu of payment recipients' actual account and routing information.
- The further the Bureau deviates from information currently provided for asset accounts and for credit and debit card accounts on periodic statements and online banking portals, the more burdensome, costly, problematic, and risky the provision of that data is likely to be.

Information Regarding Prior Transactions and Deposits That Have Not Yet Settled

- TCH does not anticipate issues with the provision of information covered in this section of the SBREFA Outline as long as the Bureau recognizes and makes allowance for the fact that provisional amounts of transactions may significantly differ from the amounts that are ultimately settled, if the transactions are settled at all.

Other Information About Prior Transactions Not Typically Shown on Periodic Statements or Portals

- The provision of information covered in this section of the SBREFA Outline would be highly problematic. This is especially true for the name and account number of the payment recipient, which could be used to facilitate fraud, should not be widely shared, and would place a large cost upon data providers. It could also be confusing to consumers. The Bureau's section 1033 rule should not require data providers to share data on prior

transactions that data providers typically do not display on account statements or through their online portals.

Online Banking Transactions That the Consumer Has Set Up But That Have Not Yet Occurred

- The information covered in this section of the SBREFA Outline is generally already made available to consumers through their banks' online banking portals. The information is, however, subject to change as it relates to transactions that have not yet occurred. Therefore, data providers that provide this information should not be held liable for issues arising from subsequent changes to scheduled transactions after the consumer's data request is made. In addition, bill payment information is highly sensitive, with the potential to reveal intimate details of a consumer's life. The sharing of bill payment information with third parties should be approached cautiously.

Account Identity Information

- The information covered in this section of the SBREFA Outline constitutes the most sensitive personally identifiable information ("PII") that a consumer has; the release of such data is inherently prone to fraud and misuse. Other than information that may be needed to prove account ownership for specific use cases (e.g., name, address, email address, telephone number), third parties can and should be required to obtain this information directly from consumers rather than data providers.
- Requiring data providers to support APIs that confirm or deny user-submitted identity information would be complex and would not produce sufficient consumer benefits to warrant the cost.

Other Information

- The Bureau should not include consumer reports in data that financial institution ("FI") covered data providers should be required to provide. Consumers can obtain consumer reports directly from consumer reporting agencies. Consumer reports that may have been obtained by FI covered data providers would be of limited utility to third parties as the latter are unlikely to rely on dated reports for their underwriting decisions.
- The proposed provision of information regarding security breaches is highly problematic as FI data providers are already subject to numerous federal and state data breach notification laws and requirements and the Bureau's proposal would impose significant additional costs on FI data providers. In addition, information regarding security breaches is beyond the scope of section 1033.

Statutory Exceptions to Making Information Available

Confidential Information

- The exception for confidential information should include information that a covered data provider has taken steps to protect, including commercially sensitive trade secrets, where disclosure would help a competitor in the market and the information is not otherwise disclosed to consumers.

- The protection from disclosure of confidential information should extend to the use of artificial intelligence and other methods by third parties to reverse engineer such confidential information based on the extraction of large quantities of consumer data. The Bureau should specifically prohibit reverse engineering.
- The exception for confidential information should extend to information that is licensed by the data provider under contractual terms that prevent its disclosure to third parties.

Information Collected for the Purpose of Preventing Fraud or Money Laundering or for Detecting or Reporting Other Unlawful or Potentially Unlawful Conduct

- Section 1033 exempts, from the general requirement to make information available, information that a data provider has collected for the purpose of preventing fraud or money laundering or for detecting or making any report regarding other unlawful or potentially unlawful conduct. The Bureau should interpret the phrase "for the purpose of" as meaning "specifically for the purpose of" (i.e., the information has no other use than the prevention of fraud, money laundering, or detecting or reporting other unlawful or potentially unlawful conduct) as opposed to the Bureau's proposal that it interpret the phrase as requiring that the information be "actually used" for the prevention of fraud, money laundering, etc.

Information Required to Be Kept Confidential by Other Law

- In considering the scope of the statutory exclusion for information required to be kept confidential by other law, the Bureau should incorporate important state law requirements, which may include contract law, privacy law, and others.

Information That Cannot Be Retrieved in the Ordinary Course of Business

- The phrase "ordinary course of business" in section 1033 should be interpreted by the Bureau to mean "typically provided by that data provider to consumers of that product or service as part of the usual course of business, custom, or practice of the institution, such as information typically provided to consumers in a periodic statement or through an account management portal."

Current and Historical Information

- The Bureau should interpret the scope of current data that a covered data provider must make available to mean only that information it has consistent with its standard posting times and other procedures adopted for handling data in the ordinary course of its business.
- Regarding historical data, covered data providers should be required to make available information only as far back in time as they make transaction history available directly to consumers.

How and When Information Would Need to Be Made Available

- The Bureau should pursue a principles-based approach that would provide high-level guidance so private-sector standard-setting bodies like FDX could develop and maintain detailed market-driven data format standards to facilitate the information exchange required by section 1033.

Direct Access by Consumers

- Consumer authentication for direct access should comport with how a data provider authenticates consumers for its internet banking portal (or, in the case of nonbanks, other service portal) in the ordinary course of its business.
- Available formats for the export of information may vary among covered data providers. Consistent with section 1033, covered data providers should be required to make information available to consumers only in whatever format they use in the ordinary course of their business for the specific information requested.

Third-Party Access

- The Bureau indicates that it is considering adopting detailed service level agreement ("SLA")-like standards for data portals. Such requirements are unnecessary and would be duplicative for FIs. Data providers that are regulated FIs are already subject to voluminous, detailed regulatory requirements regarding operational performance and operational resilience and are supervised and examined for their compliance with those requirements. Additional and potentially conflicting requirements from the Bureau would be of dubious value, would create regulatory confusion, and would substantially increase compliance complexity and cost.
- Data providers should not be required to meet higher standards for components such as availability and uptime for a third-party channel (where a customer is not always "present" in the flow) than the first-party digital channel for customers (where the customer is always present in the flow).
- Regarding the type of evidence of revocation that a data provider should receive before a third party's access to a consumer's data is terminated, TCH recommends that the Bureau adopt a flexible approach so data providers can react to properly authenticated customer requests or evidence of fraud.
- Third parties should be required to specify the use case for which they are requesting data and to comply with industry standards that outline the data fields appropriate for that use case.
- Data providers should be permitted to establish reasonable time, place, and manner restrictions in order to protect consumers and infrastructure.
- Because FI data providers will need to meet prudential regulatory requirements regarding the authentication of and access by third parties to FI systems, TCH recommends that the Bureau adopt a flexible framework in which third-party authentication is managed by the covered data provider.
- Data providers should not be required to meet stricter requirements for data accuracy on third-party channels than on customer-direct access channels.

Certain Other Covered Data Provider Disclosure Obligations

- The Bureau indicates it is considering a rule that would require covered data providers to disclose to consumers or third parties why information is not being made available. Aspects of this proposal are highly problematic as the mere disclosure that information is being withheld because it was collected for the purpose of preventing fraud or money laundering or for detecting or making a report regarding other unlawful or potentially unlawful conduct could compromise the existence of fraud, money laundering, and other criminal investigations and would be counterproductive to consumer protection goals. In addition, there are other circumstances, such as third-party due diligence reviews, where FI data providers may be contractually prevented from disclosing the results.
- In terms of whether disclosures should be made to third parties, consumers, or both, TCH believes that the requirements should be flexible and that the determination as to which party is in the best position to receive the disclosure ought to be left to the discretion of the data provider in light of the particular circumstances.
- The development of reasonable policies and procedures with respect to explaining why information is withheld is a more reasonable approach than requiring formal disclosure and would reduce costs to covered data providers. The Bureau should include specific examples of appropriate policies and procedures in the compliance guide the Bureau will be issuing.

Third-Party Obligations

Duration and Frequency of Third-Party Access

- The industry should be empowered, through FDX or some other appropriate standard-setting body, to set reasonable standards on duration and frequency by use case, subject to a regulatorily defined maximum.
- Reauthorization should be required before an authorization lapses, and there should be no grace period. The authorization and reauthorization process must be able to be automated in order for the process to be scalable.

Revoking Third Party Authorization

- The ability to easily revoke consumer consent is fundamental to ensuring consumer control; it should be as easy for consumers to revoke authorization as it is to give authorization.
- Data providers should be empowered to provide consumers with a mechanism by which they may revoke third-party authorizations. Revocation that takes place at the data provider is preferable in that the data provider can properly authenticate the consumer and communicate accurately about the scope of access and implications of revocation. Nonetheless, if the Bureau determines that revocation should take place at the third party, then it will be important that such revocation be immediately transmitted to the data provider so that both the data provider and the third party are in synch.
- Current technology allows consumers to turn off data access by entity, not typically by use case. To limit cost and ensure feasible implementation, the Bureau should pursue a proposal for turning off data access that is in line with current technology.

Limits on Secondary Use of Consumer-Authorized Information

- TCH believes the Bureau should adopt a nuanced approach to secondary use cases, with riskier secondary uses requiring affirmative consumer opt-in and less risky secondary uses requiring consumer opt-out.

Limits on Retention

- Authorized third parties should be required to delete consumer information that is no longer reasonably necessary to provide the requested product or service. Third parties should be permitted to retain consumer information beyond receipt of the consumer's revocation request only where required by law; even then, third parties should be required to disclose to consumers that the information is being retained. There should be no circumstance sufficient to justify a third party's retention of consumer credentials. De-identified information should be treated the same as all other consumer information.

Data Security

- The best way to prevent authorized third parties from exposing consumers to harm arising from inadequate data security and to ensure the consistent protection of data across the data-sharing ecosystem is to apply the Safeguards Guidelines developed by the prudential regulatory agencies to all participants in the ecosystem. In addition, third-party participants need to be subject to active supervision and enforcement if there is to be meaningful consumer protection.

Data Accuracy and 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 data user. 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 must be a part of any regulatory framework the Bureau adopts in implementing section 1033.

Disclosures Related to Third-Party Obligations

- Third parties should be required to provide a standing disclosure of how to revoke authorization that is clear and conspicuous.
- Standing disclosures should also include the extent and purposes of the third party's access to consumer data; consumers need to have this information to make informed decisions whether to continue or revoke their authorization.

Record Retention Obligations

- Authorized third parties should be required to maintain policies and procedures to comply with their obligations under any rule the Bureau issues.

Implementation Period

- Given the potential breadth of options the Bureau is considering and uncertainty as to the scope of the Bureau's proposal, it is difficult, if not impossible, to provide meaningful input on an appropriate implementation period. To the extent the Bureau develops a final rule that is consistent with current industry practices for API-related data access, implementation could be comparatively swift, particularly if small institutions leverage the efficiencies provided by utilities like Akoya. To the extent, however, the Bureau develops a final rule that materially departs from current industry practices for API-related data access, the implementation period would need to be comparatively—and substantially—longer.

Potential Impacts on Small Entities

- To the extent the Bureau enlarges the scope of covered data providers to comply with the statutory mandate, the number of covered data providers that are small entities will be substantially enlarged.
- Smaller institutions may be able to leverage industry utilities like Akoya to realize efficiencies that will bring associated cost savings.
- The scope of data potentially covered by a CFPB rule as set out in the SBREFA Outline extends well beyond that which is currently provided in periodic statements and through account management portals. Any delta between current market practices and the Bureau's requirements would substantially increase the costs of compliance.
- The cost estimates outlined by the Bureau seem extremely low and not consistent with costs incurred by entities that have already enabled API access. The Bureau should engage with data providers that are currently providing API access to ensure real-world figures are being used to estimate costs.
- The Bureau's estimate of costs likely to be incurred in developing policies, procedures, and disclosures seems to contemplate only the legal resources needed for drafting. In reality, the creation of policies, procedures, and disclosures requires the involvement of cross-functional teams, with representatives from Product, Legal, Operations, Risk Management, and Compliance. As such, TCH believes that the Bureau's cost estimates related to the development of policies, procedures, and disclosures are significantly lower than what would actually be incurred.

II. Principles for Consumer-Authorized Financial Data Sharing and Aggregation

The Bureau's most important work to date on issues relating to section 1033 of the Dodd-Frank Act has been the development and release of the Principles in October 2017. The Principles, which took into consideration feedback provided by a wide range of stakeholders in response to the Bureau's prior request for information, 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.[6] The Principles were "intended to help foster the

[6] *See* Press Release, CFPB, CFPB Outlines Principles For Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017).

development of innovative financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives."[7] 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 previously expressed vision, and remain highly relevant today.

Since the Principles were released in 2017, much has been accomplished by the industry as it has worked toward 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. To continue the industry's momentum, it is imperative that any further action taken by the Bureau be consistent with its 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 conflicting standards, inconsistent expectations or guidance, and potential bifurcation of the market into various regulatory silos, which could leave gaps in consumer protection and greatly inhibit the scalability of industry standards, utilities, and other solutions.

III. Industry Initiatives

A. TCH Connected Banking Initiative

TCH's Connected Banking initiative has worked to enable "innovation and customer control through a more secure exchange of financial data."[8] The initiative recognizes the need to move beyond a system of credential-based data access and screen scraping to a safer, more secure, more transparent, and consumer-centric API environment that benefits consumers regardless of where they interact with financial service providers.

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 to their internet banking platforms to move money, make payments, and initiate other financial transactions and services. When a consumer shares their login credentials, FI data providers may not be able to distinguish whether the login credentials are being used by the consumer, an authorized third party, or a fraudster. Data aggregators and other third parties seem to recognize this is risky. TCH has found a number of data aggregator and data user agreements that expressly *prohibit* the data aggregator's or data user's

[7] *Id.*

[8] *See* THE CLEARING HOUSE, CONNECTED BANKING: ENABLING INNOVATION AND CUSTOMER CONTROL THROUGH A MORE SECURE EXCHANGE OF FINANCIAL DATA 5 (Mar. 2020). Detailed information regarding TCH's Connected Banking initiative is available at https://www.theclearinghouse.org/connected-banking.

customers from sharing their internet platform login credentials with third parties.[9] No doubt these entities worry about threats to their own data security and integrity.

Similarly, the process of screen scraping 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 provider website. In most circumstances, scraping collects far more data than is needed to power the product or service the consumer has chosen to use. This can include PII or other details that the consumer might not have authorized if the process were more transparent to, and more capable of being controlled by, the consumer. In addition, screen scraping is more prone to inaccuracies than APIs are and has the potential of creating operational challenges for FI data providers because the process isn't managed in a predefined way, thus opening the possibility of unlimited scope or frequency of data requests. These operational challenges can draw resources away from consumer-facing platforms and create operational risk for data providers.

APIs offer significant advantages to consumers and the overall marketplace in comparison to credential-based data access and screen scraping. As the CFPB previously noted in its taskforce report on federal consumer financial law:

> An API is a structured data feed that connects the account holder, such as the consumer's bank, to the data aggregator. 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 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 provide 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.[10]

To facilitate the shift from credential-based access and screen scraping to APIs, TCH and its sister company, TCH PayCo, have actively engaged in the development of new technology standards, infrastructure, innovative solutions to address risk management requirements and legal

[9] *See, e.g.,* Robinhood Financial LLC & Robinhood Securities, LLC, Customer Agreement, sec. 5. Account Security" (revised Sept. 30, 2022) (customer is responsible for keeping account username, password, PIN, and other account details "safe and secret at all times").

[10] TASKFORCE ON FEDERAL FINANCIAL CONSUMER LAW, CFPB, TASKFORCE ON FEDERAL CONSUMER FINANCIAL LAW (VOL. I) 496 (Jan. 2021) (hereinafter "Taskforce Report") (footnote omitted). TCH has taken notice of the disclaimer with which the CFPB has prefaced the Taskforce Report regarding violations of the Federal Advisory Committee Act.

agreements and in ongoing industry collaboration.[11] The initiative is guided by the goal of acting "in the best interest of consumers [to] enhance safety and foster efficiency in financial services."[12]

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

- Model Data Access Agreement: To enhance control over the data consumers share with third parties and to provide for a safer, more secure method to facilitate such sharing, the Connected Banking initiative has focused on accelerating the ability of data providers, data aggregators, and data recipients[13] to establish safe and secure direct connections through APIs. Recognizing that legal agreements between data providers and third parties can take considerable time and resources to develop, TCH, in collaboration with its member banks and in consultation with data aggregators and data recipients, developed a model data access agreement that can be used as a reference to facilitate the development of API-related data-sharing agreements. The model agreement was specifically developed to be consistent with the Principles and focuses on consumer control and transparency, data safety and security, and appropriate accountability for risks introduced into the system.[14]
- 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.[15] More detailed information on the work of FDX is provided in section B below.
- Uniform Assessment Instrument: Meeting regulatory expectations[16] for due diligence on third parties with whom an FI data provider is sharing data (either through an API or otherwise) can be burdensome. Due diligence takes time and

[11] Some of the work TCH has done in this area was specifically acknowledged in the Taskforce Report. *See id.* at 495, n.139 (citing TCH-developed model data access agreement).

[12] *Why Connected Banking?*, THE CLEARING HOUSE, https://www.theclearinghouse.org/connected-banking.

[13] For purposes of the SBREFA Outline, the CFPB has defined "data provider" as a "covered person with control or possession of consumer financial data," a "data recipient" as a "third party that uses consumer-authorized information access to provide (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer," and "data aggregator" as "an entity that supports data recipients and data providers in enabling authorized information access." For purposes of the SBREFA Outline, the CFPB refers to data recipients and data aggregators, generally, as "third parties." SBREFA Outline, *supra* note 5, at 5, n.9.

[14] More information on the model agreement is available at https://www.theclearinghouse.org/connected-banking/model-agreement. While bilateral agreements may be needed for some time, it is anticipated that smaller 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 (described more fully in section C below), to develop common rule sets or agreements that could take the place of some or all of the content that is covered in bilateral agreements today.

[15] *See* Press Release, The Clearing House, The Clearing House Supports Financial Data Exchange Work on API Technical Standards (Oct. 18, 2018).

[16] *See, e.g.*, OCC, *Third-Party Relationships: Risk Management Guidance*, OCC Bulletin 2013-29 (Oct. 30, 2013); OCC, *Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, OCC Bulletin 2020-10 (Mar. 5, 2020). FAQ 4 of OCC Bulletin 2020-10 relates specifically to data aggregation relationships.

resources for both the FI performing it and the third party on whom it is performed. In addition, historically, each FI ended up performing one-off due diligence inquiries. To create efficiencies and encourage the development of API relationships, TCH developed a uniform assessment instrument to streamline due diligence. The instrument permits assessment vendors to collect due diligence information once and to then share it with multiple FIs through the vendor's 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 spinoff and creation of Akoya LLC ("Akoya") from the parent company of 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 playing in the market is discussed in more detail in section C 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:
    - Consumers want more education about, 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 that access persists, and what use application service providers can make of their information.[17]

B. FDX

FDX is an international, nonprofit organization operating in the United States and Canada that is dedicated to unifying the financial industry around the 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 currently comprises 231 data providers (i.e., financial institutions), data recipients (i.e., third-party financial technology companies and financial institutions[18]), 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 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 transition the industry away from credential-based access and screen

[17] *See* THE CLEARING HOUSE, CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY 3 (Nov. 2019).

[18] Many FIs are both data providers and data recipients.

scraping and enhances the security and reliability of the flow of user-permissioned data between data providers and third parties. Moving the industry to API-based access is important for a number of reasons. Most important, the use of credential-based access and screen scraping requires the sharing of sensitive consumer login credentials and provides limited, if any, 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' networks due to the sheer number of automated logins. Consumers and financial institutions also bear significant risks associated with potential data breaches at third parties and the potential for losses if fraudsters come into possession of their login credentials and other sensitive consumer information.

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 by their own financial institution and to permission only the data 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 likely have remained fragmented—using incompatible APIs, processes, and definitions. As a result of the development of the FDX API, and the efforts of TCH members to make consumer data available via API, over 42 million U.S. consumers have already been transitioned away from credential-based access and screen scraping to a version of the FDX API, allowing consumers access to their data more securely and transparently. This work is a testament to how well the market has worked in generating safe, secure solutions to consumer data sharing. We urge the Bureau to tread carefully as it develops personal financial data right regulations so as to not disrupt the significant progress the industry has achieved to benefit consumers. The CFPB should not try to jettison or supplant standards that already exist, work well, are broadly used in the market today, and are consistent with the well-considered and longstanding Principles.

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

- FDX API Specification: Currently at version 5.2, the FDX API offers the ability to access over 660 different financial data elements, including banking, tax, insurance, and investment data, making it one of the most comprehensive connected finance standards in the world. The FDX API utilizes foundational and globally interoperable standards for security, authentication, data transfer, authorization, API architecture, and identity, thereby establishing a global best-in-class solution set for user-permissioned data sharing.
- User Experience & Consent Guidelines: The FDX 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 should be given to consumers to ensure a consistent data-sharing experience regardless of where their data is held or with whom they are seeking to share it, making data sharing more consumer friendly.
- 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 common set of terms 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 to provide a given product or service. FDX-approved use cases are developed with input and feedback from a wide array of data providers, recipients, aggregators, and others and are therefore backed by strong industry consensus. Approved 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 use cases for credit management and servicing, personal financial management, account owner verification certification, and account linking for payments certification (aka money movement).
- 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 technical compatibility/interoperability before they are marketed as compliant products or acquire certain intellectual property rights. Work continues on FDX's certification platform, with separate certification standards for data providers, data recipients, and data access platforms (i.e., data aggregators and other ecosystem utilities) anticipated in early 2023.
- Global Registry: FDX has created a registry of trusted organizations 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. The registry enables those operating within the FDX ecosystem and other ecosystems to reliably identify and verify certified and/or member organizations. The FDX Registry prototype is viewable at https://registry.financialdataexchange.org/. FDX intends the registry to act as a nonprofit, noncommercial, technology-agnostic, multitenant, cross-sector, international resource.
- Reference Implementation: FDX has created a baseline model instance of the technical stack for its members to review and interact with as they implement their own FDX API instances. The technical stack is accessible at: https://developer.financialdataexchange.org/.

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 nonprofit industry standards body, also provides large incumbents and small startups alike with a level playing field on which to compete. If continued innovation is to thrive and if consumers are to continue to enjoy safe, optimized access to their financial data, it is vital that the CFPB's rulemaking in this area not impede the significant progress achieved by FDX. Indeed, we believe FDX has largely drawn a roadmap for a responsible way to protect personal financial data rights.

C. Akoya

While the development of API standards such as those developed by FDX play a critical role, standards still need to be technically implemented through API connectivity. Without the creation of one or more unifying utilities, each data provider needs to establish individual connectivity with each data aggregator or data recipient. This one-to-one model, which would require a data recipient to establish a connection with every data provider its customers use (potentially *thousands* of entities) is a practical impossibility. Connections between data holders and data providers can be made more efficient by establishing one or more unifying utilities, thereby reducing barriers to entry across the marketplace. Scale is important for achieving the greatest efficiency in such cases. Accordingly, TCH and its members have made substantial investments and progress toward scale by spinning out one such unifying utility known as Akoya from its parent company, FMR L.L.C..[19] Akoya solves for the inefficiencies of the one-to-one model by providing a one-to-many architecture, whereby each data provider can reach any Akoya-connected third party through a single API connection with Akoya. Data aggregators, data recipients, and data providers alike all have the opportunity to benefit from integrating only once with unifying utilities like Akoya to be able to securely exchange consumer-permissioned financial data with one another. The efficiency offered to the market by firms such as Akoya may be particularly beneficial to small businesses, such as smaller financial institutions and their third-party service providers, as they seek to implement API-based data-sharing capabilities.

In addition, utilities such as Akoya facilitate the control, transparency, safety, and security that the Bureau rightfully appears to envision for the data aggregation space. For example, consumers using Akoya never give out their usernames and passwords (or credentials); instead, they log in directly with their data provider to authenticate and then grant access to a data aggregator or data recipient. This puts consumers in full control of their data. Further, Akoya is fully compliant with the FDX API specification and does not retain any of the data that passes through its network. Members of the Akoya 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 access to their data through an interface provided by their FI data provider. These qualities, which have been built into Akoya since its inception, fully align with the Principles and allow Akoya to serve as a real-world model as the Bureau considers how to ensure consumer-permissioned data access puts consumer interests at the fore.

IV. Related Statues and Regulations (Questions 1–4)

The Bureau requests input on whether any of the requirements of the closely related statutes and regulations identified in Appendix C to the SBREFA Outline duplicate, overlap, or conflict with the proposals under consideration and whether there are other statutes or regulations beyond those identified in Appendix C that would duplicate, overlap, or conflict.[20] All the statutes

[19] Akoya was created to eliminate the risks associated with credential-based access and screen scraping and give people a safe, secure, and transparent way to provide access to their financial data. Akoya replaces screen scraping with APIs, enabling individuals to share their data with fintech apps using their financial institutions' existing online portals. This eliminates the need for login information to be held and stored by anyone else. Additionally, Akoya provides a simple way for people to grant, modify, or revoke access to their financial data at any time. *See Our Mission*, AKOYA, https://akoya.com/about. Additional information about Akoya is available at https://akoya.com/.

[20] The statutes and regulations identified in Appendix C to the SBREFA Outline are EFTA (15 U.S.C. §§ 1693–1693r) and its implementing regulation, Regulation E (12 C.F.R. pt. 1005); FCRA (15 U.S.C. §§ 1681–1681x) and its implementing

and regulations in Appendix C duplicate or overlap the Bureaus proposals to some degree. Of greater concern is potential conflict. These issues are discussed below.

A. EFTA/Regulation E and TILA/Regulation Z

The potential interplay between EFTA and the Bureau's implementing regulation, Regulation E, and TILA and the Bureau's implementing regulation, Regulation Z, present similar issues and are therefore being discussed together. EFTA and Regulation E afford protection to consumers in connection with their use of electronic fund transfers by imposing obligations on financial institutions with respect to disclosures, the provision of ongoing reporting and statements to consumers, and rights of consumers to resolve unauthorized transfers or errors. TILA and Regulation Z afford protection to consumers in connection with their acquisition and use of credit by imposing obligations on creditors with respect to advertising credit offers, disclosures about the cost of credit, and affording consumers resolution rights in connection with billing errors.

There is substantial overlap in the data that must be provided to consumers under EFTA/Regulation E and TILA/Regulation Z and the data that is subject to the Bureau's proposals for implementing section 1033 of the Dodd-Frank Act. While the proposals would require "covered data providers" to make available to consumers and "authorized third parties" more information than is required to be included in periodic statements and other mandated disclosures under EFTA/Regulation E and TILA/Regulation Z, there does not appear to be any direct conflict between EFTA/Regulation E and TILA/Regulation Z on the one hand and the proposals based on what the Bureau has outlined to date on the other.

The Bureau has indicated, however, that it is considering incorporating into its rulemaking certain consumer rights regarding "inaccurate data."[21] Depending on how the Bureau proceeds, this aspect of its rulemaking could be problematic. TCH strongly believes that EFTA/Regulation E and TILA/Regulation Z should continue to exclusively govern the substantive rights of consumers and the obligations of financial institutions in connection with electronic fund transfers and credit cards and credit card accounts as to what constitutes an error and responsibilities related to error resolution. There is no indication in section 1033 of the Dodd-Frank Act that Congress intended the Bureau to have the power, in the context of writing rules to implement section 1033, to upset the carefully crafted liability frameworks set forth in EFTA and TILA.

B. TISA/Regulation DD and RESPA/Regulation X

TISA and the Bureau's implementing regulation, Regulation DD, require depository institutions to disclose certain information related to savings, checking, certificate of deposit, money market, and variable-rate accounts, among others. RESPA and the Bureau's implementing Regulation X require certain covered entities to provide various disclosures and adhere to certain error-resolution standards related to mortgage loan servicing. While there is overlap between the data required to be made available to consumers under TISA/Regulation DD and RESPA/Regulation X on the one hand and the data that is subject to the Bureau's proposals for implementing section

regulation, Regulation V (12 C.F.R. pt. 1022); GLBA (15 U.S.C. §§ 6801–6809) and its implementing regulation, Regulation P (12 C.F.R. pt. 1016); TILA (15 U.S.C. §§ 1601–1667f) and its implementing regulation, Regulation Z (12 C.F.R. pt. 1026); TISA (12 U.S.C. §§ 4301–4313) and its implementing regulation, Regulation DD (12 C.F.R. pt. 1030); and RESPA (12 U.S.C. §§ 2601–2617) and its implementing regulation, Regulation X (12 C.F.R. pt. 1024).

[21] *See* SBREFA Outline, *supra* note 5, at 46–47.

1033 of the Dodd-Frank Act on the other, there does not appear to be any direct conflict between the two.

As stated above, however, the Bureau has indicated it is considering incorporating certain consumer rights regarding "inaccurate data" into its rulemaking.[22] Similar to the issues raised with EFTA/Regulation E and TILA/Regulation Z above, TCH believes firmly that TISA/Regulation DD and RESPA/Regulation X should continue to exclusively govern the obligations of depository institutions and other covered entities to identify and correct any inaccurate data. There is simply no indication in section 1033 of the Dodd-Frank Act that Congress intended the Bureau to have the power in the context of its rulemaking to implement section 1033 to alter the carefully considered framework of rights set forth in TISA and RESPA.

C. FCRA/Regulation V

FCRA and the Bureau's implementing regulation, Regulation V, require that data collected by consumer reporting agencies from entities that furnish information be accurate to ensure that individuals are not improperly denied services, products, or employment on the basis of false information. Consumers are entitled to obtain copies of their credit scores and credit files, and there are provisions for error resolution. FCRA and Regulation V also impose limitations on the use of data and disclosures to third parties.

The Bureau's proposals are not sufficiently definite to allow TCH to fully evaluate the potential conflict between the proposals and FCRA/Regulation V. The Bureau has, however, indicated that consumer reports from consumer reporting agencies could be among the data that covered data providers would be required to make available. As TCH discusses more fully on page 36 below, TCH believes that consumers and authorized third parties should obtain such data directly from consumer reporting agencies. This would help ensure the data is appropriately current and usable. To the extent the Bureau nonetheless decides to move forward with this aspect of the proposal, there may need to be amendments to FCRA/Regulation V to permit such information sharing. The Bureau has also indicated it is considering incorporating into its rulemaking certain consumer rights regarding "inaccurate data." Similar to the points made above, TCH strongly believes that FCRA/Regulation V should continue to exclusively govern consumer rights with respect to data accuracy and error resolution concerning data collected and reported by consumer reporting agencies.

In addition, there is a need to clarify the extent to which FCRA itself applies to permissioned data and what obligations, if any, are imposed on various stakeholders. TCH submits that FI data providers cannot and should not be subject to FCRA requirements relating to furnishers of information.[23] FI data providers are not in the position of actively providing the data but are mere conduits for information that is being pulled by the data aggregator or data user acting as their customer's agent.[24] FI data providers will not generally know the purposes for which data is being

[22] *See id.*

[23] *See* Kwamina Williford & Brian Goodrich, *Why Data Sources Aren't Furnishers Under Credit Report Regs*, LAW360 (Sept. 25, 2019).

[24] Such a result is consistent with Regulation V, which specifically excepts consumers 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

pulled by a data aggregator or data user or how it may be manipulated, used, or displayed once it is out of the FI's possession. Further, requiring FIs to take on the obligations of furnishers under FCRA has the potential to clash with the clear parameters of section 1033, which requires FIs to make available only that information that is in their "control or possession" and which specifically excepts "any information that the covered person cannot retrieve in the ordinary course of its business…."[25] Section 1033 requires that a data provider disclose the data 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.

D. GLBA/Regulation P

Under GLBA and the Bureau's implementing regulation, Regulation P, a financial institution is generally prohibited from disclosing nonpublic personal information ("NPI") about a consumer to nonaffiliated third parties unless the institution satisfies various notice and opt-out requirements and the consumer has not opted out of the disclosure. Under Regulation P, a consumer cannot prevent the sharing of NPI by an FI with affiliated and nonaffiliated third parties in certain contexts, which include the disclosure of NPI to any third party with the consumer's explicit consent, provided that the consumer is given an opportunity to later revoke consent by reasonable means.[26]

The Bureau indicates it is considering requiring data providers to make available highly sensitive PII related to the identity and characteristics of the consumer account holder. For the reasons more fully discussed by TCH on pages 35–36 below, TCH believes that such information is beyond the scope of section 1033 of the Dodd-Frank Act and, because of its highly sensitive nature, is best provided by the consumer directly to the third party.

If the Bureau nonetheless decides to move forward with this aspect of the proposal, the framework of GLBA and Regulation P, including liability provisions associated with violations, strongly suggests that authorization should take place at the data provider, not at the third party as the Bureau seems to envision. This is because the only way a data provider would be reasonably assured the consumer's authorization (i.e., explicit consent) is valid and in accordance with the requirements of GLBA and Regulation P would be if the authorization takes place at the data provider.

TCH further notes that the Bureau is considering proposing that data providers provide some form of authorization disclosure that would include the identity of intended data recipients to whom information may be disclosed and the purpose for which information is being accessed.[27] This aspect of the proposal suggests that, for financial institutions subject to Regulation P, the Bureau would need to harmonize or integrate the authorization disclosure requirements under that regulation with whatever rules the Bureau implements pursuant to section 1033 to ensure

aggregator or data user, the consumer should be the one viewed as ultimately providing the information to the data aggregator or user, and the exception from the furnisher definition should apply.

[25] *See* 12 U.S.C. §§ 5533(a); 5533(b)(4).

[26] *See* 12 C.F.R. § 1016.15(a)(1).

[27] *See* SBREFA Outline, *supra* note 5, at 16.

consistency of the required disclosures.[28] As it develops more detail concerning its proposals, the Bureau should review the sample disclosure forms set out in Regulation P for use by covered financial institutions, including the "opt-out notice," to ensure they are consistent with any final rule the Bureau implements under section 1033.

E. OCC and Other Agency Guidance on Third-Party Risk Management

In addition to the issues noted above, the OCC and other federal financial services regulatory agencies have issued detailed guidance on third-party risk management.[29] The various bulletins issued by the agencies set forth detailed expectations "for assessing and managing risks associated with third-party relationships," including risk management and oversight of third party relationships "throughout the life cycle of the relationship."[30] The OCC, in particular, has noted that such guidance is specifically applicable to relationships with data aggregators and that banks have a responsibility "to manage these relationships in a safe and sound manner with consumer protections."[31]

The OCC has further made clear that risk management expectations apply *regardless* of whether the bank has a formal relationship with the data aggregator or whether the data aggregator is accessing the bank's systems independently through screen scraping and the use of customer access credentials:

> Information security and the safeguarding of sensitive customer data should be a key focus for a bank's third-party risk management when a bank is contemplating or has a business arrangement with a data aggregator. A security breach at the data aggregator could compromise numerous customer banking credentials and sensitive customer information, causing harm to the bank's customers and potentially causing reputation and security risk and financial liability for the bank.
>
> If a bank is not receiving a direct service from a data aggregator and if there is no business arrangement, banks still have risk from sharing customer-permissioned data with a data aggregator. Bank management should perform due diligence to evaluate the business experience and reputation of the data aggregator to gain assurance that the data aggregator maintains controls to safeguard sensitive customer data.[32]

---

[28] This would be similar to the process the Bureau followed to integrate the disclosures required under RESPA and TILA with respect to mortgage lending. *See* Integrated Mortgage Disclosures Under the Real Estate Settlement Procedures Act (Regulation X) and the Truth in Lending Act (Regulation Z), 78 Fed. Reg. 79730 (Dec. 31, 2013).

[29] *See*, *for example*, OCC Bulletin 2013-29, *supra* note 16 (supplemented by OCC Bulletin 2020-10, also *supra* note 16); Board of Governors of the Federal Reserve System, *Guidance on Managing Outsourcing Risk*, SR 13-19/CA 13-21 ((Dec. 5, 2013; updated Feb. 26, 2021); FDIC, *Guidance for Managing Third-Party Risk*, FIL-44-2008 (June 6, 2008). The three agencies have proposed interagency guidance to replace this guidance. *See* Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38182 (proposed July 19, 2021).

[30] See, e.g., OCC Bulletin 2013-29, *supra* note 16.

[31] *See* OCC Bulletin 2020-10, FAQ 4, *supra* note 16.

[32] *Id.*

The SBREFA Outline does not mention agency guidance on third-party risk management, so it is unclear how mandates that the CFPB is considering in its rulemaking will accommodate the OCC and other agency guidance on this important issue.[33] As just noted, under current OCC guidance, responsible banks seek to gain a level of assurance that the data aggregator maintains controls to safeguard sensitive consumer data. If data providers are required to provide data to any consumer-authorized data aggregator or other third party without qualification, it is unclear how banks could comply with both the OCC's guidance and the requirements the CFPB has outlined.

Banks have legitimate interests in protecting their customers and their systems. They also must adhere to regulatory and supervisory obligations across their various regulators and supervisors. It is crucial, therefore, that the CFPB make appropriate accommodations in any rulemaking for banking agency guidance on third-party risk management. Specifically, and as required by section 1033(e)(1) of the Dodd-Frank Act,[34] the CFPB should ensure its rulemaking is consistent with requirements of the federal banking regulators and recognize that third-party risk management obligations require financial institution data providers to manage who can access consumer-permissioned account information and implement reasonable contractual obligations on those entities (e.g., data security, data use, liability, audit/oversight).

V. Coverage of Data Providers Subject to the Proposals Under Consideration (Questions 5–8)

The SBREFA Outline suggests that the CFPB is considering a rule that, if finalized, would require only a limited, defined subset of all covered persons to make consumer financial information available to a consumer or an authorized third party, notwithstanding the broad language of section 1033(a). Specifically, the CFPB is considering limiting data providers to covered persons that meet the definition of "financial institution" in Regulation E or "card issuer" in Regulation Z.[35]

The practical effect of this proposed limitation would be the likely inclusion of all or almost all depository financial institutions and a select few fintech payment providers (e.g., PayPal, Venmo, and others that provide some form of "account" and electronic fund transfer services or that issue credit cards that relate to an open-end (not home-secured) consumer credit plan). That would mean data would regularly flow from well-regulated depository financial institutions to a vast array of third-party fintech entities, most of which are unregulated or, at best, lightly regulated. As outlined, these third-party fintech entities appear to extend well beyond the defined subset of institutions that would be required to provide data, further bifurcating the consumer financial marketplace. Such an approach is at odds with the statutory language of section 1033 of the Dodd-

[33] The Bureau notes that it has "invited discussion" on the SBREFA Outline from staff at the Board of Governors of the Federal Reserve System, the OCC, the FDIC, and other agencies and that it "plans to continue conferring with these and other agencies throughout the rulemaking process." SBREFA Outline, *supra* note 5, at 8, n.20.

[34] 12 U.S.C. § 5533(e).

[35] Regulation E defines a "financial institution" as "a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services [other than persons excluded from coverage by section 1029 of the Dodd-Frank Act]." 12 C.F.R. § 1005.2(i). Regulation Z defines "card issuer" as "a person that issues a credit card or that person's agent with respect to the card." 12 C.F.R. § 1026(a)(7).

Frank Act, inconsistent with advancing the competition goals the CFPB has articulated as being a driving force behind its proposed rulemaking, and likely to severely diminish the data-sharing universe the private sector has already created. Perversely, and perhaps unintentionally, the net effect of the proposed limitation would be to harm consumers by constricting the data access that many consumers enjoy as a result of the private sector's earlier efforts.

The statutory language in section 1033 of the Dodd-Frank Act does not support the approach the CFPB is considering. Section 1033 requires that "a covered person shall 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 …."[36] The term "covered person" is defined in the Dodd-Frank Act to mean any person that engages in offering or providing a consumer financial product or service and any affiliate of any such person if such affiliate acts as a service provider to such person.[37] "Consumer financial product or service" is also a defined term and means any financial product or service defined under the Dodd-Frank Act that is offered or provided for use by consumers primarily for personal, family, or household purposes or delivered, offered, or provided in connection with certain financial products or services (namely, extending credit or servicing loans, providing real estate settlement services or appraising loans, performing certain credit report-related activities, and collecting consumer debt).[38] Section 1033 therefore encompasses a broad array of financial service providers, well beyond those the SBREFA Outline considers covered data providers, including financial services providers involved in extending credit (home/auto loans), financial advisory services, brokerage and retirement accounts, buy-now, pay-later ("BNPL") installment loans, crypto wallets, and providers of financial data products and services. The scope of "covered person" in section 1033, having been defined by Congress, should not be redefined and limited by the Bureau. To the extent any rulemaking differs from the requirements of section 1033, it may raise significant legal questions as to the validity of the final rule.

In addition, the limitations being considered by the CFPB in its SBREFA Outline are at odds with its stated goals, which the CFPB notes are to "bolster[] consumers' right to access personal financial data and, if they wish, share their data with others, including competing financial services users."[39] The ability to do so is intended to "intensify competition in consumer finance" and "enhance competition and drive better service aimed at keeping customers."[40] These broad goals are ill served by a proposal that omits a majority of the consumer financial services market and would deprive consumers of the full benefits that section 1033 of the Dodd-Frank Act was intended to achieve, including control of their data across the financial services marketplace.

The SBREFA Outline also does not consider certain accounts that may fall under the definition as outlined but that are owned by minors. There are specific protections and features of these and other accounts that may unintentionally be included.

---

[36] Dodd-Frank Act § 1033(a) (codified at 12 U.S.C. § 5533(a)).

[37] 12 U.S.C. § 5481(6).

[38] 12 U.S.C. § 5481(5). The definition of "financial product or service" can be found at 12 U.S.C. § 5481(15).

[39] *See* SBREFA Outline, *supra* note 5, at 4.

[40] *Id.*

Last, the private sector has already created an extensive data-sharing ecosystem, mutually benefiting consumers and a broad range of financial service providers, that includes the ability to share data from a far broader array of entities than the CFPB is considering in the SBREFA Outline. It is unclear whether these other entities would continue to be willing to participate in the data-sharing ecosystem if they were clearly excluded from the Bureau's section 1033 rulemaking. Consumers therefore risk being harmed by a rule that would diminish the scope of the existing data-sharing ecosystem. To take just one example, would consumers find it satisfactory if, when using their personal financial management tool (a core data-sharing use case today), they were unable to access account information about retirement funds held at a brokerage firm, liabilities such as mortgage and auto loans, BNPL purchases, assets held in a crypto wallet, or other financial products outside those specified in the SBREFA Outline?

Consistent with the broad data rights noted above that Congress envisioned in enacting section 1033, equal access to data sharing across financial service providers is necessary both for full consumer benefit and a level playing field. Only then will a truly competitive marketplace emerge, one that allows consumers to decide which products and services best meets their needs. To facilitate fair competition and recognize the consumer benefits intended by Congress as set forth in section 1033, only entities that are engaged in providing a consumer financial product or service on a truly de minimis basis should be exempt from its requirements.

VI. Recipients of Information

A. Direct Access by Consumers (Question 11)

Section 1033(a) of the Dodd-Frank Act generally requires data providers to make information available directly to "a consumer." Regardless of section 1033 requirements, consumers already have broad electronic access today to their financial information, with access being facilitated by data providers through online banking platforms and a host of other tools, including many third parties.

The CFPB is considering how its proposals should address a covered data provider's obligation to make information available directly to a consumer when the account is held by multiple consumers. Specifically, the CFPB is "considering proposing that a covered data provider would satisfy its obligation to make information available directly to a consumer by making the information available to the consumer who requested the information or all the consumers on a jointly held account."[41]

TCH appreciates the flexibility embodied in that proposal and observes that a one-size-fits-all approach to this issue would not likely succeed, making flexibility paramount. Different types of accounts may have very different account terms, differing legal requirements, and very different authorization requirements and responsibilities associated with them. Who has authority to request and receive information associated with different types of accounts must be left to the discretion of data providers working with their customers to find the kind of account relationship that best fits the customer's needs and existing legal requirements.

Finally, given the important relationship that a consumer has with their financial institution, coupled with the inherent risks associated with sharing sensitive consumer data with unaffiliated

[41] SBREFA Outline, *supra* note 5, at 14.

third parties, the CFPB, as part of any rulemaking, should strongly encourage the direct transfer of any data to the consumer, as contemplated as part of section 1033.

B. Third-Party Access

In addition to making information available directly to a consumer, the Dodd-Frank Act includes in the definition of "consumer" an agent, trustee, or representative acting on behalf of an individual.[42] Although not specifically defined as part of section 1033 or otherwise cross-referenced, if the definition of "consumer" as set forth in 12 U.S.C. § 5481 is applied, the effect is to require data providers to make information available, upon request, to authorized third parties.

1. Authorization Procedure, Disclosure, Timing, and Format (Questions 12–20)

Authorization is fundamental to ensuring consumer control over their information and to protecting the ecosystem from fraud and other illegal or unauthorized activity. The Bureau is considering a proposal that would include a requirement that, in order to access consumer information under the rule, the third party accessing the information would need to (1) provide an "authorization disclosure" to inform the consumer of key terms of access; (2) obtain the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and (3) certify to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information.[43] The authorization disclosure would contain information on the key scope of access that "might include" the general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, and how to revoke access.[44] The authorization disclosure would also contain key use terms that "might include" the identity of intended data recipients (including any downstream parties) and data aggregators to whom the information may be disclosed and the purpose for accessing the information.[45] As outlined, the third party would be required to provide the authorization disclosure "close in time" to when it would need the consumer-authorized information to provide the product or service requested by the consumer.[46] A third party would be required to obtain consent in writing or electronic form, evidenced by the consumer's signature or the electronic equivalent, and the Bureau is further considering proposing that a third party would be required to provide consumers a copy of their signed consent, either electronically or through the mail.[47]

TCH notes that the proposal is in some ways less detailed than the Bureau's prior statements on authorization and disclosure set forth in the Principles. Given the amount of work that the industry has done to conform existing data access practices to the Principles, it is critical that any future rulemaking conform in all material respects to the Principles, which have generally worked well in practice. Specifically, Principle 3 outlines detailed criteria for consumer consent and authorization.

---

[42] 12 U.S.C. § 5481(4).

[43] SBREFA Outline, *supra* note 5, at 15.

[44] *Id.* at 16.

[45] *Id.*

[46] *Id.*

[47] *Id.* at 17.

> 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 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.[48]

The Bureau should develop optional model disclosure forms for all parties that are consistent with Principle 3 and could provide a safe harbor.[49] Disclosure requirements should apply to both data providers and third parties. Those requirements must reflect, however, that FI data providers will have limited visibility into data usage and downstream parties once the data leaves the provider. Accordingly, the obligation on data providers should generally be limited to disclosing (1) to whom the data is initially and directly provided, (2) the fact that the provision of data was authorized, and (3) identification of the appropriate mechanism by which the consumer may halt the ongoing provision of data. Data providers should be provided with sufficient flexibility in how they obtain and capture the customer's authorization via the data provider's online portal and/or API.

To ensure consumers are in control of their 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 may be accessed and for what purpose, and for how long it is being stored. Disclosures must be sufficiently clear and easily understood by consumers to ensure that their authorization is knowingly given. Disclosures should also clearly spell out the consumer's right to revoke authorization and should include the right to be forgotten, with instructions on how to invoke those rights that are no more onerous than what is required to initially grant authorization. The Bureau should prohibit the sale of consumer data unrelated to the direct provision of any authorized product or service to the consumer.

The regulatory framework will also need to address authorization requirements with disclosures that are segregated and sufficiently clear and easily understood by consumers to ensure their authorization is knowingly given. 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

[48] Principles, *supra* note 4, at 3.

[49] TCH notes that the Bureau may wish to examine precedents such as the model disclosures and disclosure templates in the prepaid account rule (https://www.consumerfinance.gov/compliance/compliance-resources/consumer-cards-resources/prepaid-cards/prepaid-model-forms-samples/) and disclosures such as the Schumer box relating to TILA (https://www.consumerfinance.gov/rules-policy/regulations/1026/g/).

forget they have signed up for a particular service.[50] Accordingly, data providers should have the right to build API services in a way that allows the consumer to control the flow of data and the scope of authorization at the data provider.

To ensure consumers continue to wish to provide their data, data providers should have the right to set reasonable periodic reauthorization requirements that work for the data provider and its customers. This is how the market works today, with the reasonableness of reauthorization requirements subject to market discipline. Too short a reauthorization requirement will lead to a bad customer experience and customer attrition. Data providers are therefore incented to impose reasonable requirements, consistent with their ability to protect their systems and their customers. In the event, however, that the Bureau does not provide for authorization at the data provider, it should establish a periodic reauthorization requirement of reasonably short duration, with reauthorization required more frequently after a period of nonuse (e.g., 90 days).[51]

To ensure meaningful compliance among similarly situated market participants, any regulatory framework developed by the Bureau must ensure appropriate supervision and enforcement based on the risks posed to consumers through a larger participant rulemaking or other assertion of supervisory authority.[52]

The SBREFA Outline fails to address what rights and protections, if any, a consumer would have if a data recipient initiates a cross-border transfer of the consumer's data once the data recipient is in possession of that data. This may be a fundamental concern to consumers in their management of their data and could raise significant security concerns.

The SBREFA Outline appears to contemplate an authorization process that takes place at third parties. Most TCH members believe that authorization at third parties is at odds with how well-functioning authorization in an API environment is accomplished today.[53] The FDX API specification already lays out detailed standards relating to secure authentication and authorization.[54] In the FDX authorization standard, the data provider is notified when the third party seeks access to the consumer's data. The data provider then requests that the consumer establish proof of identity directly with the data provider, which typically is accomplished when the consumer presents a username and password known only to the consumer and the data provider.

---

[50] *See generally* CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY, *supra* note 17.

[51] A bank would ordinarily expire token access and require a consumer to reauthorize the access every 90 days by reentering their credentials. Such steps are fundamental to maintaining account security. Further, the CFPB should consider instituting a presumption of revocation (rather than reauthorization) when circumstances indicate the consumer is no longer interested in participating in the third-party service (e.g., if they fail to log in or to fund the account for a period).

[52] *See* Letter from American Bankers Association *et al.* to CFPB (Aug. 2, 2022) (petition for rulemaking defining larger participants of the aggregation services market).

[53] TCH notes that technology regarding authorization may evolve and suggests that the issue of authorization be further analyzed and discussed by the Bureau with stakeholders before further proposals are iterated.

[54] *See* FINANCIAL DATA EXCHANGE, THE GLOBAL INDUSTRY STANDARD FOR CONSUMER ACCESS TO FINANCIAL DATA (released Aug. 29, 2019). The FDX authorization standard is based on widely used standards developed over several years of industry collaboration by the Internet Engineering Task Force (IETF) and the OpenID Foundation. The FDX authorization standard is also based on the OAuth 2.0 authorization framework, OpenID Connect and the Financial-grade API Security Profile, which have benefited from extensive, formal security analysis and the yearslong collaborative efforts of industry security experts.

After the consumer's identity is verified, the consumer confirms to the data provider the scope of data authorized for the third party's access. The data provider then authorizes the access of the third party to the consumer's data through an API maintained by the data provider for the purpose of sharing data with third parties. Such an approach is not only critical for addressing fraud prevention, but also allows financial institutions to comply with third party risk management requirements.

The Bureau's rule should not disrupt the significant progress the industry has made on this and other issues to the benefit of consumers. Authorization at third parties is not only a known vector for fraud (indistinguishable from credential sharing) but is at odds with the well-functioning authorization paradigm in today's FDX API environment, a standard that covers more than 42 million consumers and multiple applications.[55] As mentioned above, FDX has also developed detailed user experience guidelines for the implementation of consumer dashboards at data providers and third parties. The FDX standard aligns with and facilitates globally interoperable standards, which are important to scaling the financial data-sharing ecosystem. The failure to align the Bureau's rulemaking with existing standards that are widely used to facilitate data sharing today—and which are consistent with the Principles—would impose substantial and unnecessary retooling costs on the industry and would result in a much less safe and secure data-sharing environment.

Providing for authorization to take place at the data provider is also fundamental to achieving the Bureau's aspirations in Principle 8—namely, that consumers have a reasonable, practical means to dispute and resolve instances of unauthorized access and data sharing, unauthorized payments that result from unauthorized data sharing, and failures to comply with other obligations, such as the terms of consumer authorizations.[56] As long as consumers are required to give out their login IDs and passwords to third parties to facilitate data access and as long as screen scraping exists, it will be substantially difficult, if not impossible, for data providers to resolve unauthorized access claims in favor of the consumer as the process of credential-based access and screen scraping limits the FI data provider's visibility into what data had been authorized and for whom. Tokenized access through an API is the surest method through which an FI data provider can appropriately validate authorization. Consequently, the abolition of credential-based access and screen scraping is fundamental to the achievement of the Bureau's vision as articulated in Principle 8.

The Bureau has asked for comments on authorization procedures where a data recipient relies on a data aggregator to access consumer data from the data provider. Specifically, the Bureau has asked whether third-party obligations should apply to the data recipient, the data aggregator, or both. TCH believes that a consumer would expect and deserve disclosure by both the data aggregator and the data recipient of the terms pursuant to which they will handle and use the consumer's data. Since both will be handling the consumer's data and since how they handle and use that data may fundamentally vary, both should be required to make the relevant disclosures.

Additionally, the Bureau has asked for comments on how to address authorizations where a covered account is held by more than one consumer. As discussed above on page 25, joint accounts

[55] *See* Press Release, Financial Data Exchange, LLC, Financial Data Exchange (FDX) Reports 42 Million Consumer Accounts on FDX API to Continue Driving Open Banking (Oct. 31, 2022).

[56] *See* Principles, *supra* note 4, at 4.

can raise significant issues. Who has authority to authorize the disclosure of information should be left to the discretion of data providers working with their customers to find the kind of account relationship that best fits the customer's needs. If, however, the Bureau decides to be prescriptive, it should create a safe harbor for data providers from other claims if they act in conformance with what the Bureau specifies. In addition, the SBREFA Outline suggests other specific account types that have additional legal protections, such as accounts for minors, might be covered.

The Bureau has also asked if there are any circumstances in which more limited disclosures would be appropriate. TCH does not believe that there are such circumstances. Consumers have a right to control the use and disclosure of their data. Full disclosure of the use being made of data by third parties is a substantial component of consumer protection.

Regarding timing, the Bureau has suggested that disclosures should be provided "close in time" to when the third party would need the consumer-authorized information. TCH notes that "close in time" is inherently ambiguous and further could be interpreted to be either before or after data access. TCH believes that a better standard would be to require disclosure immediately prior to authorization by the consumer. By receiving the disclosures immediately prior to authorization, consumers would be in the best position to evaluate and understand the use of their data prior to the introduction of risks inherently associated with data transfer.

2. Certification Statement

The Bureau is considering proposals under which, to be authorized to access consumer information, a third party would be required to certify to the consumer that it will abide by certain obligations regarding use, collection, and retention of the consumer's information. The CFPB has requested comment on whether the full certification statement should be included in the authorization disclosure.

It is unclear from the SBREFA Outline what purpose the certification statement would be intended to fulfill, particularly in light of the disclosure statement that the Bureau has indicated would also be required to be provided. Based on what is stated in the SBREFA Outline, although TCH does not believe the certification statement would be harmful, it is difficult to comment definitively without more fully understanding the intended additive value of the certification. For instance, would such a certification confer any additional rights on consumers or impose additional obligations on third parties beyond those that might be set out in a final rule? A certification is only likely to be an effective consumer protection tool if it confers on consumers clear rights against any data acquirer, aggregator, or downstream user.

VII. Types of Information a Covered Data Provider Would Be Required to Make Available (Questions 22–38)

Subject to certain exceptions, section 1033 of the Dodd-Frank Act requires a covered data provider to make available to a consumer, upon request, information in its control or possession concerning the consumer financial product or service that the consumer obtained from the data provider, including information relating to any transaction, series of transactions, or the account, including costs, charges, and usage data.[57] The Bureau sets forth six categories of information—some of which go well beyond the data specified in section 1033—that the Bureau is considering

[57] 12 U.S.C. § 5533(a).

requiring covered data providers to make available with respect to covered accounts.[58] The Bureau cautions that the specific data elements set forth within each of the six categories should not be taken as exhaustive but as representative. The six categories are:

1. Periodic statement information for settled transactions and deposits;
2. Information regarding prior transactions and deposits that have not yet settled;
3. Other information about prior transactions not typically shown on periodic statements or portals;
4. Online banking transactions that the consumer has set up but that have not yet occurred;
5. Account identity information;
6. Other information.

Each category is specifically addressed below. Before doing so, however, TCH believes it is useful to consider several core concepts that should apply to data scope overall.

First, any rulemaking relating to the scope of information to be provided under section 1033 of the Dodd-Frank Act should conform to 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.[59]

TCH submits that achievement of the Bureau's vision as outlined in Principle 2 may be inhibited because of misaligned incentives. Data aggregators and data users that engage in screen scraping obtain data well beyond that which is 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 from the Bureau to sunset the practice of screen scraping, there may not be adequate incentive among market participants to transition from screen scraping to a more-controlled API environment where only the data required to provide the consumer with the service is being shared.

Second, data access must be limited by the particular use case at issue consistent with the principle of data minimization. Use cases developed by FDX could be a useful starting point. It should be noted, however, that the use cases developed by FDX are quite broad and that individual services within the overall FDX use case might have a much narrower need for data. Regardless of the technical standard, the Bureau needs to clarify, as part of any section 1033 rulemaking, that the

[58] *See* SBREFA Outline, *supra* note 5, at 18.

[59] Principles, *supra* note 4, at 3.

industry standard must be subservient to an overall data minimization principle: data aggregators and data users should obtain only those types of data they need for the product or service then being provided, and consumers should be fully in control of which categories of data are being provided, to whom, for how long, and for what purpose, regardless of use case. This level of consumer control is contingent on moving to an API environment.

Third, for consumers to be assured that a third party is accessing only the data necessary to provide the product or service and maintaining that data only for as long as necessary, they must have adequate and accurate transparency as to the nature of the product or service, what data is being accessed, for what use, by whom, and for how long. This must be coupled with appropriate regulatory oversight and supervision. The issue of data scope, therefore, is intimately tied to the issue of disclosure.

A. Periodic Statement Information for Settled Transactions and Deposits

The Bureau is considering proposing that covered data providers make available information with respect to settled transactions and deposits that generally appears on the periodic statements that covered data providers are currently required to provide for asset accounts and for credit card accounts.[60] Data elements would include the following:

1. For each transfer, the amount, date, and location of the transfer and the name of the third party (or seller) to or from whom the transfer was made;
2. Any fees charged to the account;
3. Any interest credited to an asset account or charged to a credit card account;
4. The annual percentage yield of an asset account or the annual percentage rate of a credit card account;
5. The current account balance;
6. The account balance at the beginning and at the close of the statement period, as well as, for credit card accounts, upcoming bill information (including whether a payment is overdue or the account is delinquent);
7. The terms and conditions of the account, including a schedule of fees that may be charged to the account;
8. For an asset account, the total dollar amount of all charges for paying overdraft items and for returning items unpaid, both for the statement period and for the calendar year to date, as required by Regulation DD; and
9. For an asset account, the account number as required by Regulation E.[61]

TCH notes that all this information is made available today by TCH members through their online banking portals, consistent with existing regulations, and through existing authorized third-party data-sharing relationships that are being facilitated by TCH members. Accordingly, TCH does not generally anticipate issues for data providers to make the identified data elements available so

[60] SBREFA Outline, *supra* note 5, at 19.

[61] *Id.* at 19–20.

long as it is done pursuant to an API and a defined use case scenario. A rule on data access that allows unfettered access without an API and defined use case scenarios is inconsistent with the principles of consumer control and would render ineffective the acquisition of informed consent. Moreover, any final rulemaking should make clear that data providers should have the option of sharing tokenized account numbers and routing numbers with authorized third parties in lieu of payment recipients' actual account and routing information. The financial services industry is shifting toward the tokenization of payment-related information to provide greater customer protection and control and lower instances of fraud. TCH's sister company, TCH PayCo, has led the industry in efforts to shift toward tokenization of account and routing numbers through its Secure Token Exchange.[62] Data tokenization and future security improvements made by market participants in an effort to protect consumers and reduce fraud should be embraced by the Bureau and recognized as important implementations in the final rule. Otherwise, a rule *requiring* data providers to share actual account and routing information would introduce unnecessary risk into the payments ecosystem.

Additionally, TCH notes, the further the Bureau deviates from information currently provided for asset accounts and for credit and debit card accounts on periodic statements and online banking portals, the more burdensome, costly, problematic, and risky the provision of that data is likely to be. New processes, definitions, and data feeds would need to be created, likely at significant cost, to facilitate the sharing of such data. Such deviation would likely be particularly burdensome for small institutions that may not have the technological ability or resources to create or modify such processes and data feeds in-house.

B. Information Regarding Prior Transactions and Deposits That Have Not Yet Settled

The Bureau is considering proposing that covered data providers make available information regarding transactions and deposits that have not yet settled. The Bureau notes this might include data about transactions by the consumer that the covered data provider has approved, or agreed to pay, but that have not yet settled, as well as data about deposits to an asset account, or payments to a credit card account, that have not settled or might not be available to the consumer to use.[63] TCH does not anticipate issues with the provision of this information as long as the Bureau recognizes and makes allowance for the fact that provisional amounts may significantly differ from the amounts that ultimately settle, if they settle at all. Hotels, gas stations, and rental car agencies, for example, may make provisional charges to a credit card or deposit holds that ultimately differ from or are not part of the settled amount. In addition, payments and credits that are provisionally applied may be corrected prior to settlement. The Bureau should provide that, where data providers make the information available at the time the data request is processed, they will not be held responsible if amounts indicated differ from the actual amounts settled or if the amounts never settle.

C. Other Information About Prior Transactions Not Typically Shown on Periodic Statements or Portals

The Bureau is considering proposing that covered data providers make available information about prior transactions that covered data providers typically do not include on

[62] *See generally Secure Token Exchange,* THE CLEARING HOUSE, https://www.theclearinghouse.org/payment-systems/Secure-Token-Exchange.

[63] SBREFA Outline, *supra* note 5, at 20.

periodic statements or through online financial account management portals but that are received from payment networks.[64] The Bureau indicates that such data may include "elements regarding the interbank routing of a transaction," which might indicate "the bank into which a card, ACH, or check transaction was deposited by a merchant or other payee, such as a fraudster" and "the name and account number at that bank of the merchant or other payee (such as a fraudster) that deposited the payment transaction" and might further indicate "which banks in between the merchant's bank and the consumer's bank handled the transaction."[65] The Bureau argues that such information "may be useful to a consumer or an authorized third party seeking to resolve a dispute with, or recover funds from, a fraudster or the fraudster's bank."[66] This statement is speculative and without support.

TCH believes that the disclosure of this information, especially the name and account number of the payment recipient, would be highly problematic. Accordingly, TCH advocates for a final rule that does not require data providers to share data on prior transactions that the data providers typically do not display on account statements or through their online portals. First, names and account numbers can be used to facilitate fraud and should not be widely shared. Additionally, the proposed disclosure of this information would place a large cost upon data providers and would be confusing to customers. Despite this, the Bureau has not clarified what the associated consumer benefit would be for sharing this level of information (such as information on all the parties involved in processing an ACH debit).

The Bureau specifically seeks information about the length of time for which covered data providers retain detailed transaction information or can obtain the information from the relevant payment network. It should be noted that retention periods for such data vary significantly between institutions and networks—there is no uniform retention period. For certain data elements, however, data providers can provide information consistent with the applicable regulatory timelines in Regulations E and Z—generally two years.[67]

D. Online Banking Transactions That the Consumer Has Set Up But That Have Not Yet Occurred

The Bureau is considering proposing that covered data providers make available information regarding banking transactions a consumer has set up but that have not yet occurred.[68] Data might include information about a biller with which the consumer has a relationship and information relevant to that relationship, such as the consumer's account or identification number with the biller.[69] Data might also include the amounts of bills and the dates on which the consumer would like payments to be transferred.[70]

---

[64] SBREFA Outline, *supra* note 5, at 21.

[65] *Id.*

[66] *Id.*

[67] *See* 12 C.F.R. §§ 1005.13(b)(1); 1026.25(a).

[68] SBREFA Outline, *supra* note 5, at 21.

[69] *Id.*

[70] *Id.* at 22.

TCH notes that this information is generally made available to consumers through their banks' online banking portals and, currently, may also be made available to authorized third parties through data sharing arrangements facilitated by TCH members. The provision of this information, however, can be particularly complex, necessitates specific definitions, and is subject to consumer confusion. As we emphasized above, data providers that provide this information should not be held liable for issues arising from subsequent changes to scheduled transactions after the consumer's data request is made. The only obligation should be to provide information that is current as of the time of the request. In addition, bill payment information is highly sensitive, with the potential to reveal intimate details of a consumer's life. The sharing of bill payment information with third parties should be approached cautiously.

The CFPB should also keep in mind that sharing biller information is separate and distinct from accessing or changing biller information, as section 1033 does not grant third parties the ability to make "write" changes to data providers' portals. Allowing the sharing of biller information may be useful to consumers in some circumstances but also carries risk. For instance, when a consumer shares biller information with a fintech to set up autopay, they may not understand that enabling the fintech autopay does not disable the autopay they had set up earlier through their FI, leading to double payments and possibly resulting in overdrafts.

E. Account Identity Information

The Bureau is considering proposing that covered data providers make available information related to the identity and characteristics of the consumer account holder.[71] The Bureau notes that such information might include the following:

1. Name
2. Age
3. Gender
4. Marital status
5. Number of dependents
6. Race
7. Ethnicity
8. Citizenship or immigration status
9. Veteran status
10. Residential address
11. Residential phone number
12. Mobile phone number
13. Email address
14. Date of birth
15. Social Security number
16. Driver's license number

TCH notes that some of this information is the most sensitive PII that a consumer has and that the release of such data is inherently prone to fraud and misuse. For certain data elements, it is unclear what legitimate use third parties would have, so the risk of misuse seems to heavily outweigh any marginal benefits. Furthermore, third parties can easily obtain this information directly from the consumer if the consumer wishes to provide it. Indeed, requiring consumers to

[71] *Id.*

proactively provide this information to third parties is a valuable tool to ensure they are aware that any given entity has access to their sensitive personal information.

Furthermore, as it pertains to mitigation of these risks through a "confirm/deny" approach, requiring data providers to support APIs that confirm or deny user-submitted identity information would be complex and would not produce sufficient consumer benefits to warrant the cost. Existing tools that confirm or deny the "match" between user-submitted identity data across systems are difficult to operationalize in practice, and very few market participants confidently use this method in their own business applications for risk management and identity verification purposes.

Last, other than basic identity information that may be needed to confirm identity on the account based on a particular use case (e.g., name, email address, address, telephone number), this type of data is not "information . . . concerning *the consumer financial product or service*" being obtained from the data provider[72] and therefore does not fall within the purview of section 1033 of the Dodd-Frank Act. For this reason, the Bureau should not go beyond the unambiguous statutory language to include such data in its rulemaking to implement section 1033.

F. Other Information

The Bureau is considering proposing that covered data providers make available other information they might have about their consumer account holders, including:

1. Consumer reports from consumer reporting agencies;
2. Fees that covered data providers assess in connection with their covered accounts;
3. Bonuses, rewards, discounts, or other incentives; and
4. Information about security breaches that exposed a consumer's identity or financial information.[73]

TCH notes that consumer reports from reporting agencies are available directly to consumers and are of limited utility to third parties as they are unlikely to rely on dated reports for their underwriting decisions. Furthermore, data providers may be contractually prohibited from sharing consumer reports. In addition, the combination of consumer report and account terms is competitively sensitive. If a third party possessed this information, it might be able to reverse engineer the data provider's underwriting process and other confidential commercial information, creating a significant competitive disadvantage for data providers.[74] The Bureau should not include consumer reports from data providers as currently proposed in any future rulemaking to implement section 1033 of the Dodd-Frank Act.

TCH further notes that the provision of information regarding security breaches is also highly problematic as banks are already subject to numerous federal and state data breach

[72] *See* 12 U.S.C. § 5533(a) (emphasis added).

[73] SBREFA Outline, *supra* note 5, at 23.

[74] The CFPB is prohibited from requiring covered persons from disclosing confidential commercial information. 12 U.S.C. § 5533(b).

notification laws and requirements.[75] The Bureau's proposed requirement in this regard would impose significant additional costs on data providers. Furthermore, information regarding security breaches is beyond the scope of section 1033 of Dodd-Frank Act, which requires the disclosure of information "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 to the account including costs, charges and usage data."[76] Information regarding data breaches is inconsistent with the character of information called for in the statute, which focuses on transactional information. Had Congress intended for section 1033 to encompass data breach notification requirements, it would have included those requirements in the statute.

Data aggregators that experience breaches should also be held liable for damages arising from those breaches. In addition, the Bureau should include a provision that would hold data providers blameless for any information they provide in good faith in response to an authorized, or apparently authorized, data request that includes information subsequently determined to be from a fraudulent or synthetic identity account.

Although not explicitly discussed in the SBREFA Outline, to the extent the CFPB is contemplating the portability of specific account numbers (either for accounts as defined under Regulation E or for credit card accounts under Regulation Z) between financial institutions—such that, from the consumer's perspective, the account numbers do not change—there would be serious system and network challenges, as well as risks of widespread fraud and safety and soundness concerns, which would have to be fully considered and addressed across the industry.[77] The costs to introduce such a capability are likely to be extremely significant for financial institutions regardless of their size.

Finally, for all data elements that are ultimately included in the final rule, the CFPB should work with industry to ensure that data definitions are standardized across market participants and aligned with existing regulations (e.g., the definition of "fee") in order to reduce implementation frictions and costs.

G. Statutory Exceptions to Making Information Available

The Bureau seeks information as to how the exceptions set forth in section 1033 of the Dodd-Frank Act should affect the Bureau's proposals. Those exceptions state that a data provider may not be required to make available:

- Confidential information, including algorithms used to derive credit scores or other risk scores or predictions;

[75] *See, e.g.,* Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021) (codified at 12 C.F.R. pt. 53 (OCC), 12 C.F.R. pt. 225 (Federal Reserve), 12 C.F.R. pt. 304 (FDIC)); CAL CIV. CODE §1798.80–.84; DEL. CODE ANN. tit. 6, §§ 12B-100 to –104; 815 ILL. COMP. STAT. 530/5–900; N.Y. GEN. BUS. LAW §§ 899-aa–899-bb.

[76] *See* 12 U.S.C. § 5533(a).

[77] *See generally* Rohit Chopra, Director, CFPB, Prepared Remarks at Money 20/20 (Oct. 25, 2022) (discussing Federal Communications Commission's telephone number portability rules).

- 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 or data application subject to patent, trademark, copyright, or trade secret protection developed by the data provider or acquired from a third party intended for display or use only within the data provider's portal;
- Any information required to be kept confidential by any other provision of law; or
- Any information that the data provider cannot retrieve in the ordinary course of its business.[78]

1. Confidential Information

TCH believes that the exception for confidential information should include information that a covered data provider has taken steps to protect, including commercially sensitive trade secrets, where disclosure would help a competitor in the market and the information is not otherwise disclosed to consumers. This would include but would not be limited to custom scores, underwriting models, underwriting criteria, and other confidential and proprietary information that is not shared with consumers.

The exception should extend to the use of artificial intelligence and other methods by third parties to reverse engineer such confidential information based on the extraction of large quantities of consumer data. We acknowledge that costs, charges, and other terms under which financial products and services are provided to consumers and offers made to individual consumers that are disclosed to them are 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 provider to conduct its business. Notably, prohibiting such reverse engineering would be similar to the provisions frequently found today in data aggregator and data user agreements that bar those accessing *their* services from using the data they provide to reverse engineer their own proprietary systems and processes.[79] In addition to the clear language of section 1033, the risk of big data aggregation to a competitive marketplace further demonstrates why the Bureau should prioritize the sharing of consumer data directly to consumers themselves when they request it.

[78] 12 U.S.C. § 5533(b).

[79] *See*, *e.g.*, *Terms of Use*, ACORNS GROW INC., https://www.acorns.com/terms/ (updated May 13, 2020) (prohibiting reverse engineering, decompiling, or otherwise translating Acorns content or user interface material); *Terms of Use*, MX TECHNOLOGIES INC., https://www.mx.com/terms/ (updated Jan. 15, 2020) (prohibiting, without express prior written consent, reverse engineering, decompiling, altering, modifying, disassembling, or otherwise attempting to derive source code used in MX services or any third-party applications incorporated into MX services); *End User Privacy Policy*, PLAID INC., https://plaid.com/legal/ (effective Feb. 22, 2022) (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); *User Agreement*, PAYPAL, INC., https://venmo.com/legal/us-user-agreement/ (effective Sept. 14, 2022) (providing that users agree not to engage in numerous activities, including modifying, altering, tampering with, repairing, reverse engineering, translating, disassembling, or decompiling, relating to source code derived from Venmo software or any third-party materials or technology that are incorporated).

The Bureau should clarify, as part of any rulemaking, that such reverse engineering is inconsistent with section 1033's intent and is not an appropriate use of the data for the purpose of providing the product or service to the consumer.

Finally, information that is licensed by the data provider under contractual terms that prevent its disclosure to third parties should also fall within the category of confidential information that is excepted from disclosure.

2. Information Collected for the Purpose of Preventing Fraud or Money Laundering or Detecting or Reporting Other Unlawful or Potentially Unlawful Conduct

Section 1033 of the Dodd-Frank Act exempts, from the general requirement to make information available to a consumer, information a data provider has collected for the purpose of preventing fraud or money laundering or for detecting or making any report regarding other unlawful or potentially unlawful conduct. The Bureau is considering whether it should interpret "for the purpose of" to generally mean information that a covered data provider *actually* uses to prevent fraud or money laundering or to detect or report potentially unlawful conduct or that the covered data provider would not have collected but for a legal requirement to collect the information for these purposes.[80]

TCH believes that such an interpretation is overly restrictive and not in keeping with the intent of section 1033, which is to allow institutions to freely collect information for the purpose of preventing wrongful conduct. For example, fraud risk scores, which are widely used by the industry, would arguably need to be disclosed under the CFPB's proposed definition if they did not specifically result in a transaction denial, but nevertheless are clearly used to reduce fraud risks in the marketplace. TCH believes a better interpretation of "for the purpose of" is "specifically for the purpose of" (i.e., the information has no other use than the prevention of fraud, money laundering, or detecting or reporting other unlawful or potentially unlawful conduct).

3. Information Required to Be Kept Confidential by Other Law

Section 1033 of the Dodd-Frank Act also states that a data provider may not be required by that section to make available any information required to be kept confidential by any other provision of the law.[81] The Bureau is considering whether it should interpret "information required to be kept confidential by any other provision of law" to generally mean "information subject to a statutory or regulatory requirement to keep the information confidential from the consumer who obtained the consumer financial product or service to which the information pertains."[82] TCH believes such an interpretation is generally reasonable, though the CFPB should ensure its interpretation covers important state law requirements, such as contract law, privacy law, and others, to ensure that data providers are not forced to violate applicable state law.

[80] *See* SBREFA Outline, *supra* note 5, at 25.

[81] 12 U.S.C. § 5533(b)(3).

[82] SBREFA Outline, *supra* note 5, at 26.

4. Information That Cannot Be Retrieved in the Ordinary Course of Business

Section 1033 also makes clear that a data provider may not be required by that section to make available any information that the data provider cannot retrieve in the ordinary course of its business.[83] The Bureau believes that the phrase "ordinary course of business" is particularly ambiguous and seeks information as to how it should interpret the phrase. TCH believes that the phrase "ordinary course of business" should be interpreted to mean "typically provided by that data provider to consumers of that product or service as part of the usual course of business, custom, or practice of the institution, such as information typically provided to consumers in periodic statements or through an account management portal." Circumstances where a data provider must engage in additional back-end research for data, although the data provider might have the data, should fall within the statutory exemption. To go beyond such a definition to require other information would be very costly and burdensome, particularly for small businesses and institutions.

5. Current and Historical Information

The CFPB is considering proposing that a covered data provider make available the most current information that the covered data provider has in its control or possession at the time of a request for current information.[84]

TCH believes that it is important, however, to interpret the provision of current data consistent with the statutory parameters set by Congress in section 1033. Congress wisely sought to minimize the burdens imposed on data providers by limiting the obligation of data providers to provide only that information that is in their "control or possession" and by further specifying that data providers not be required to make available any information that they could not retrieve in the "ordinary course of business."[85] Consistent with these important limitations, the Bureau in any rulemaking should interpret the scope of current data that a covered data provider must make available to mean only that information it has consistent with its standard posting times and other procedures adopted for handling data in the ordinary course of its business.

With respect to historical information, the Bureau notes that section 1033 "shall not be construed to impose a duty on a data provider to maintain or keep any information about a consumer."[86] In light of the statutory language in section 1033, the Bureau is considering a proposal under which a covered data provider would be required to make available only information as far back in time as that covered data provider makes transaction history available directly to consumers.[87] TCH believes that this approach is reasonable as long as it is interpreted to mean that a data provider must provide data only for as long as that specific data is provided directly to consumers.

---

[83] 12 U.S.C. § 5533(b)(4).

[84] SBREFA Outline, *supra* note 5, at 27.

[85] *See* 12 U.S.C. §§ 5533(a); 5533(b)(4).

[86] SBREFA Outline, *supra* note 5, at 27 (referring to 12 U.S.C. § 5533(c)).

[87] SBREFA Outline, *supra* note 5, at 27.

VIII. How and When Information Would Need to Be Made Available

The Bureau describes proposals related to how and when a covered data provider would need to make information available in part III.D of the SBREFA Outline. The Bureau notes that section 1033(a) of the Dodd-Frank Act states that a data provider shall make information available in an electronic form usable by consumers and, further, that section 1033(d) provides that "[t]he Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section."[88]

It should be noted that while section 1033 requires the Bureau to address standardized formats for data 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…."[89] 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 FDX could develop and maintain detailed market-driven standards to facilitate the information exchange required by section 1033. TCH believes that a market-driven approach to the development and maintenance of standards is far preferable to a regulatory one. 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. Consequently, such mandated standards would have the potential to significantly slow or freeze innovation.

A. Direct Access by Consumers (Questions 39–49)

The Bureau notes that it is considering proposing that a covered data provider be required to make available information if it has enough information to (1) reasonably authenticate the consumer's identity and (2) reasonably identify the information requested.[90] TCH believes that consumer authentication should comport with how a data provider authenticates its consumer into its internet banking portal (or, in the case of nonbanks, other service portal) in the normal course of its business. Banks are subject to detailed requirements regarding customer authentication and will need to continue to comply with those requirements.

The Bureau further notes that it is considering proposing that covered data providers be required to make available all the information that would be covered by the proposals under consideration through online financial account management portals.[91] For the reasons previously set forth in sections C, E, and F of part VII of this letter, TCH believes that such a requirement would be highly problematic for several categories of information that the Bureau has proposed. In addition, to the extent any such information is not currently customarily provided through internet banking portals, the cost and expense of doing so would be excessive in light of the limited utility of the information. Further, the provision of this information to customers could create a confusing

[88] *Id.* at 28.

[89] 12 U.S.C. § 5533(d) (emphasis added).

[90] SBREFA Outline, *supra* note 5, at 28.

[91] *Id.*

and poor customer experience since customers would not otherwise ordinarily have access to that information.

The Bureau also notes that is it considering proposing that covered data providers be required to allow consumers to export the information covered by the proposals under consideration in both human and machine-readable formats.[92] TCH notes that the available formats for the export of information may vary among covered data providers. In this regard, it should be noted that section 1033 does not impose any obligation on covered data providers to create information that is not otherwise in the "control" or "possession" of the covered data provider and that section 1033 provides an explicit exception for "information that the covered person cannot retrieve in the ordinary course of its business with respect to that information."[93] Further, it would be very burdensome (from both cost and network architecture perspectives) for data providers to be required to support sharing this information in three different formats (human readable, machine readable, and via API), especially considering the limited benefits that customers would realize from such a requirement (particularly with regard to machine-readable data available via data providers' consumer portals). Consistent with section 1033, covered data providers should be required only to make information available to consumers in whatever format the data provider uses in the ordinary course of its business for the specific information requested.

The Bureau asks whether covered data providers have policies and procedures in place to ensure that the information made available through online account management portals is not made inaccurate due to the way the portal operates or the way the information is transmitted to the consumer. Banks have such policies and procedures and are regulated and supervised for operational performance. Bank platforms go through substantial testing prior to operationalization with bank customers to ensure the platforms are reliable and perform in accordance with specifications.

The Bureau seeks information on alternative means by which covered data providers could satisfy their obligations under the rule. Specifically, the Bureau requests information on channels other than online financial account management portals through which covered data providers make information available electronically to consumers. TCH notes that not all channels are amenable to handling all information and that it will be important for the Bureau to provide flexibility to covered data providers to meet their obligations. Currently, the channels used by covered data providers to make information available electronically to consumers include email, SMS, push notifications, and particularized financial applications. Consumers must be properly authenticated before information is provided through any channel, and the provision of information must align with state and federal privacy laws.

The Bureau seeks information on how covered data providers authenticate a consumer's identity when making information available other than through an online financial account management portal. Banks use various means to authenticate their customers depending on the channel and are highly regulated and supervised for cyber and data security, including with respect to methods of authentication. Methods include multifactor authentication, tokens, out-of-band

[92] *Id.*

[93] *See* 12 U.S.C. §§ 5533(a); 5533(b)(4).

messaging, validation of customer phone numbers, and customer verification of certain elements of PII that they have provided to the data provider.

The Bureau seeks information on how data providers define the scope of information requested by consumers through channels other than online financial account management portals and whether there are circumstances in which covered data providers encounter overly burdensome requests. Generally, this is a customer service issue for a bank data provider; defining the scope of information requested will depend on the nature of the information. If the bank has data relating to the consumer and the data does not fall within one of the exceptions outlined in section 1033, the requested data will generally be provided (assuming the data requested falls within the bank's retention period).

B. Third-Party Access

The Bureau lays out a number of proposals for third-party access in part III.D(2) of the SBREFA Outline.

1. Obligation to Make Information Available Through a Data Portal (Questions 50–56)

The Bureau is considering proposing that covered data providers be required to make information available, upon request, to third parties authorized to access information on a consumer's behalf.[94] The Bureau is also considering what role screen scraping should play in the context of a covered data provider's compliance with the rule.[95] The Bureau is rightly "concerned that screen scraping presents some significant limitations and risks to consumers, data providers, and third parties, including risks related to possession of a consumer's credentials."[96] The Bureau is therefore considering proposing that covered data providers be required to establish and maintain a third-party portal that does not require the authorized third party to possess or retain consumer credentials.

TCH believes that any rulemaking by the Bureau should include a specific ban on screen scraping. 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 storage and 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. Screen scraping also poses risks related to the scope of data being scraped, operational risks for data providers, and risks to consumers resulting from diminished control over the data being accessed. Therefore, credential-based access and screen scraping should be abolished. There may, however, be little incentive for data aggregators and data users to halt these practices given that (1) APIs offer data access that is limited by the consented-to use case, consumer controlled, and transparent, (2) API access will necessarily subject data aggregators

[94] SBREFA Outline, *supra* note 5, at 30.

[95] *Id.* at 31.

[96] *Id.* at 31.

and data users to some level of risk management due diligence,[97] and (3) API access will impose upon data aggregators and data users certain costs associated with building and maintaining API connectivity. There is substantial consumer benefit, however, in hastening the transition away from credential-based data access and screen scraping and to more secure methods like APIs. These benefits include but are not limited to more transparency for consumers about who is accessing their data, elimination of overcollection of data by data recipients and data aggregators, greater control by consumers over authorization and revocation, greater protection of consumer data from fraud or theft, and the provision of access to 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 that prohibits data aggregators and data users from obtaining consumer data using a consumer's online banking credentials and screen scraping where a data provider has provided the data aggregator or data user with the option of enabling API access. Given the consumer risk associated with screen scraping, the ban on scraping should go beyond the narrow definition of "covered accounts" and encompass the practice in its entirety.

The Bureau will undoubtedly need to phase in such an approach. Most large financial institutions already have some form of data-sharing API connectivity. Smaller institutions may need more time but can leverage industry utilities like Akoya. It will therefore be important that any rule allow covered data providers to provide APIs either directly or indirectly.

A phased approach could define different classes of covered data providers subject to different implementation periods based on asset size or customer base. Defining classes by customer base would have the added benefit of providing protection as rapidly as possible to the greatest number of consumers. Determining an appropriate period for implementation by each class needs substantially more research and a more definitive proposal than the Bureau has outlined at present. For example, implementation could be relatively rapid if the data fields are limited to those most commonly used by third parties today (including account balances, transactions, account details, and account holder information). Significantly more work (and consequently time) would be required if data sharing were extended to data beyond what third parties most commonly use today.

The Bureau has inquired as to whether covered data providers should be required to permit screen scraping when the covered data provider's third-party access portal experiences a service interruption. TCH members are all highly regulated and supervised financial institutions. Regulation and supervision extend to operational performance and resiliency, ensuring that our member institutions provide a high level of uptime and consistent system performance. While all systems need some downtime for maintenance and software and hardware updates, disruption should be minimal. Whatever minimal disruption occurs is not sufficient to justify screen scraping and credential-based access and the plethora of risks those practices entail. Instead, once API access is made available to a third party, that third party should be required to delete any and all information, including consumer credentials, associated with or gained through screen scraping. Allowing third parties to hold credentials for any reason, including as a backup option to APIs, not only reintroduces all the risks inherent to credential-based access but also fails to honor consumers' authorization, as providing the ability to scrape screens in this instance would also provide third parties with unlimited access to data outside the scope, duration, and frequency that the consumers have authorized. Moreover, allowing screen scraping if a covered data provider's

[97] *See* OCC Bulletin 2020-10, *supra* note 16 (FAQs 4–7, describing agreements for sharing customer-permissioned data through APIs and risk management due diligence requirements).

third-party access portal experiences a service interruption would create a multitude of consumer experience issues. Consumers, who would likely be unaware of the service interruption, would be provided with the illusion that their data is secure when in reality the data would be subject to screen scraping, which would permit the third party to collect data beyond the scope of their initial authorization. In addition, consumers would need to both authenticate with their banks to enable API access and separately give their credentials to the third party. Such a practice would be confusing for consumers.

The Bureau has asked whether there are ways that the Bureau could mitigate the consumer risks associated with screen scraping, such as by requiring covered data providers to provide access tokens to authorized third parties. While such an approach addresses some risks associated with credential-based access, it does not address a host of other risks associated with screen scraping. Token-based access does not mitigate the risks associated with less customer control and transparency, access by a third party to more data than it needs, or data that is less timely and accurate than that obtained via API. For these reasons, credential-based access and screen scraping should be abolished without exception and the industry transitioned to safer, more secure API access. Further, in consideration of the above, if a data provider offers access to third parties via an API, that data provider should be permitted to block all screen scraping by third parties to provide its customers with maximum security. There should also be a corresponding prohibition on third parties attempting to screen-scrape any data provider that makes data available via an API, as it would be very costly for banks to effectively block screen scraping, protect customers, and enforce usage of safer APIs without such a prohibition. Indeed, in the past, data providers have witnessed highly sophisticated and ongoing efforts by third parties to make their scraping traffic "look human" to evade controls data providers have instituted to block unauthorized screen-scraping. Identifying and stopping screen-scraping requires data providers to make significant and ongoing expenditures of effort and technology investment.

2. Data Portal Requirements (Questions 57–71)

The Bureau is considering various proposals related to the availability of information obtained through third-party access portals and the impact of such portals on the accuracy of information accessed through them.[98] While the Bureau notes that it is aware that industry standard setting has led to the development and implementation of voluntary standards and guidelines, and views such activity as a "positive development," the Bureau nonetheless is "considering proposing requirements to promote the availability, security, and accuracy of information made available to authorized third parties…."[99]

While many details remain undefined, the Bureau seems to indicate that it is considering adopting detailed SLA-like standards, such as standards regarding uptime, latency, planned and unplanned outages, error response and access caps, and performance standards relating to the accurate transmission of consumer information for third-party access portals. TCH believes the approach outlined by the Bureau is highly problematic.

Data providers that are regulated financial institutions are already subject to voluminous, detailed regulatory requirements regarding operational performance and operational resiliency

[98] SBREFA Outline, *supra* note 5, at 32.

[99] *Id.*

and are supervised and examined for their compliance with those requirements.[100] Additional and potentially conflicting requirements from the Bureau would be of dubious value, would create regulatory confusion, and would substantially increase compliance complexity and cost, particularly for smaller institutions. TCH believes that performance standards should be left to prudential regulators. At most, the CFPB should adopt a principles-based approach that would be consistent with existing regulatory requirements and supervisory expectations. If, however, data providers are required to adhere to SLAs, the SLAs must be reasonable. Even then, such SLAs may impose significant costs on data providers. Accordingly, data providers should be provided with the ability to charge reasonable fees to third parties in this instance. The cost of measuring and demonstrating compliance with SLA requirements could be significant for data providers. Data providers should not be required to meet higher standards for components such as availability and uptime for a third-party data channel (where a customer is not always "present" in the flow) than their first-party digital channel for customers (where the customer *is* always present in the flow).

The Bureau notes that it is not considering proposing new or additional data security standards with respect to a covered data provider's third-party access portal (other than with respect to the method of authenticating the authorized third party).[101] This is because the Bureau "believes that nearly all —if not all—covered data providers must already comply with either the Safeguards Rule or Guidelines issued under the Gramm-Leach-Bliley Act (GLBA), as well as the prohibition against unfair practices."[102] TCH supports this approach with regard to depository financial institutions. Information security guidelines for depository financial institutions would be duplicative of existing regulatory and supervisory frameworks. By the same logic, however, the Bureau should similarly recognize that operational and resiliency requirements are also unnecessary and would be duplicative of existing regulatory requirements and supervisory expectations that the prudential regulators have established for depository financial institutions.

Regarding non-depository fintechs that are regulated under Federal Trade Commission ("FTC") authority, the supervisory and enforcement structure of the FTC is materially different than that of the prudential regulators, with the FTC generally having only "after the fact" supervisory authority and more limited enforcement authority.[103] There is a need, therefore, for more robust examination and supervision of, and enforcement over, non-depository fintech data providers that the Bureau should accomplish through the exercise of its larger participant rulemaking authority.

Additionally, to the extent additional standards are needed, TCH believes that such standard setting is best left to industry standard-setting bodies like FDX. Shifting away from the existing framework established by industry participants through FDX could damage innovation and potentially result in standards that are impractical to implement. Entities such as FDX are better able to respond to the needs of the marketplace, have strong representation from all stakeholders, and are sufficiently nimble to adjust to future technological changes as market needs evolve.

---

[100] *See, e.g.*, FFIEC, FFIEC INFORMATION TECHNOLOGY HANDBOOK: ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS (June 2021); FFIEC, FFIEC INFORMATION TECHNOLOGY HANDBOOK: BUSINESS CONTINUITY MANAGEMENT (Nov. 2019); FFIEC, FFIEC INFORMATION TECHNOLOGY HANDBOOK: INFORMATION SECURITY (Sept. 2016).

[101] *See* SBREFA Outline, *supra* note 5, at 35.

[102] *Id.* (footnote omitted).

[103] *See generally* Federal Trade Commission, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority (revised May 2021).

Finally, such detailed SLA-like standard setting would appear to be beyond the scope of the Bureau's authority as outlined in section 1033 of the Dodd-Frank Act. While section 1033 allows the Bureau to engage in a rulemaking to require covered persons to make data available, it is silent on regulating standards such as bank system uptime and performance. Indeed, Congress has already given such authority to the prudential regulators.

3. When Covered Data Providers Would Be Required to Make Information Available to Authorized Third Parties (Questions 72–84)

The Bureau is considering proposing that a covered data provider be required to make data available to a third party, upon request, when the covered data provider has received evidence of the third party's authority to access information on behalf of a consumer, information sufficient to identify the scope of the information requested, and information sufficient to authenticate the third party's identity.[104] The Bureau also notes that it is "seeking to ensure that third parties that do not meet these conditions are prevented from obtaining access to the information."[105]

As discussed more fully above, at pages 28–29, the Bureau's proposed framework for third-party authorization, which appears to envision authorization taking place at the third party and the third party forwarding that authorization to the data provider, is at odds with the Bureau's goal of ensuring that third parties that do not have authority are prevented from obtaining access. The only secure way for a data provider to confirm third-party authorization is for the consumer to be authenticated to the data provider's platform and to provide authorization directly to the data provider. This is why current API arrangements and the FDX standard are architected in that manner. The Bureau should follow a similar approach.

The Bureau requests information on the type of evidence of revocation of a third party's authorization a covered data provider should be required to receive before access is terminated. TCH recommends a flexible approach that would allow data providers to react to properly authenticated customer requests or evidence of fraud. Customers will naturally rely on their banks to protect their accounts and information; banks should be empowered to do so.

The Bureau requests comment on whether covered data providers should be required to inform consumers of which third parties are accessing information pursuant to a purported authorization. TCH believes that such a requirement is appropriate but only in an API environment. Data providers are frequently unable to distinguish consumer access from third-party access in credential-based screen-scraping environments, which is yet another reason supporting the sunset of such activity.

The Bureau notes that it is considering proposing that data providers be required to make available information in conformance with the duration, frequency, and type specified in the request made by the authorized third party.[106] The Bureau's current proposals on how consumer authorizations should be captured and operationalized in the data-sharing ecosystem are not practical in light of the principle of data minimization. Accordingly, most TCH members support an environment in which the covered data provider—not the authorized third party—manages

[104] SBREFA Outline, *supra* note 5, at 36.

[105] *Id.*

[106] SBREFA Outline, *supra* note 5, at 37.

consumer authorizations, including to define and set forth the options that make up the scope of authorization the consumer can choose to grant (e.g., on data categories, accounts). An environment in which authorized third parties would control consumer authorizations would reduce the benefits of data privacy and data minimization.

Furthermore, the Bureau should be less prescriptive and allow flexibility for market participants to build third-party data-sharing solutions that honor the customer's scope of authorization, while also balancing the principles of data minimization and technical feasibility. As noted more fully above on pages 31–32, data access must be limited by the particular use case at issue, consistent with the principle of data minimization. Additionally, there is a need to recognize the work that FDX has done to create common use cases and data categories around which data providers can build their APIs to meet the needs of the market. Third-party data requests should be required to specify the use case for which the data is being requested and comply with industry standards outlining the data fields appropriate for that use case.

Furthermore, data providers should be permitted to establish reasonable time, place, and manner restrictions. There is a risk that the cumulative volume of third-party traffic could overwhelm and negatively affect the functioning of data providers' systems, as unfettered third-party access to data providers' APIs would introduce undue and excessive burdens on data providers' infrastructure. Requiring or promoting "account mirroring" (e.g., a third party pulling data from a data provider every hour or seeking real-time updates) would not only overwhelm data providers' technology systems but would also be unnecessary as a large percentage of aggregation use cases can be supported by one data pull per day (or even less frequent pulls). As such, data providers should be permitted to place reasonable restrictions on access, including access to their own APIs, to protect their customers and infrastructure.

The Bureau also seeks input on approaches for a data provider to authenticate the third party's identity. The Bureau acknowledges that data providers have a legitimate interest in the secure handling and storage of their customers' information.[107] The Bureau is considering proposing that a covered data provider make information available to a third party upon request when it receives information sufficient to authenticate the identity of the third party. The Bureau seeks input on whether data providers should be required to follow certain specific procedures in authenticating an authorized third party's identity.

Outside of a framework of either bilateral contracts or an industry registry of authorized third parties, it would be very difficult and inefficient for data providers to operationalize the direct verification of the identity of third parties (of which there may be hundreds or thousands). Today, this objective is accomplished primarily through a series of contractual obligations between data providers, data aggregators, and data recipients. But there is no uniform process for authenticating third parties. To meet third-party risk management expectations, each financial institution would have to perform due diligence on the third parties that wish to access its systems and would, in the context of establishing a relationship with the third party, have to ensure its method of authenticating the third party's identity meets regulatory expectations. Authorizing third-party access into bank systems is already an activity for which depository financial institutions are highly

[107] *Id.* at 38.

regulated and supervised.[108] Therefore, TCH advocates for a flexible framework in which third-party authentication is managed by the covered data provider.

The Bureau seeks input on whether covered data providers should be required to make information available to third parties when they know the information requested is inaccurate. Practically speaking, to accomplish the scale of data sharing the Bureau envisions, the provision of data will need to be highly automated. Culling out potentially inaccurate data would necessarily involve a manual process, which would be inefficient, if not wholly infeasible. Further, accuracy must necessarily be judged in the context of how the data will be used, but the data provider will not have significant visibility into all the purposes for which the data might be shared. Additionally, from a cost/benefit perspective, requiring data providers to meet stricter requirements for data accuracy on third-party channels than on customer-direct access channels (such as the financial institution's online customer portal) would be not only costly for data providers but also not in the best interests of customers across all channels.

C. Certain Other Covered Data Provider Disclosure Obligations (Questions 85–87)

The Bureau notes that it is considering a rule that would require covered data providers to disclose to consumers or authorized third parties the reason information is not available pursuant to the section 1033(b) exceptions.[109] TCH believes that aspects of this proposal are profoundly problematic if it would mean disclosing information that was collected for the purpose of preventing fraud or money laundering or detecting, or making a report regarding, other unlawful or potentially unlawful conduct. The mere disclosure that information was being withheld for such purposes could compromise the existence of fraud, money laundering, and other criminal investigations and would be counterproductive to consumer protection goals.

In addition, TCH notes that information may be withheld in certain circumstances because the third party has failed to meet reasonable standards in an appropriate due diligence review.[110] Such reviews are almost always conducted pursuant to nondisclosure agreements; consequently, data providers would likely be contractually prevented from disclosing the results of those reviews.

The Bureau asks whether, with respect to disclosing why access is prevented, covered data providers should be required to provide disclosures to third parties, consumers, or both. TCH believes that the proposed requirements should be flexible and that the determination as to which party is in the best position to receive the disclosure is best left to the data provider in light of the particular circumstances.

The Bureau asks whether it would facilitate compliance or reduce costs to covered data providers if, rather than prescribe disclosures, covered data providers were required to implement reasonable policies and procedures with respect to explaining why information is withheld. TCH encourages the Bureau to provide more specific information on what it has in mind and take into account the constraints mentioned above.

---

[108] For examples of agency risk management guidance, refer to footnote 29 above.

[109] SBREFA Outline, *supra* note 5, at 39. Disclosure would, of course, have to be made contingent upon the data provider knowing there was a data request.

[110] See discussion of agency guidance on third-party risk management above at pages 22–23.

The Bureau also asks for input on whether and how covered data providers should inform consumers of rights afforded to them pursuant to the rule. It is unclear from the SBREFA Outline what specific rights the Bureau is referring to. To the extent the Bureau is referring to rights generally, TCH notes that such an exercise could be both costly for data providers and ineffective, since all consumers would presumably need to receive the notice and the timing and content of the notice would lack context. TCH further questions the value of such a notice given that consumer account agreements will necessarily have to be updated to take into account any data-sharing rule the Bureau promulgates. TCH believes the information set forth in the consumer's account agreement will necessarily be the best source of information on the data provider's responsibilities and the consumer's rights.

IX. Third-Party Obligations

The Bureau notes that it is considering proposals under which third parties accessing consumer-authorized information would have certain obligations related to the collection, use, and retention of that information and requests feedback as to those obligations.[111]

A. General Limit on Collection, Use, and Retention (Question 88)

The Bureau is considering a rule that would prohibit authorized third parties from collecting, using, or retaining consumer information beyond what is reasonably necessary to provide the product or service the consumer has requested. The Bureau appropriately notes that such a limitation standard is an appropriate way of "reducing the risks of over-collection and retention of sensitive information, including risks associated with breaches of retained information, while allowing for uses of information needed to provide consumers with the products and services that they requested."[112] The Bureau requests input on the approach it is considering to limit third-party collection, use, and retention of consumer-authorized information to what is reasonably necessary to provide the requested product or service.[113]

As noted in more detail on pages 31–32 above, TCH believes the approach the Bureau is considering to minimize the collection, use, and retention of data to only that necessary to provide the requested product or service is not only appropriate but essential to the implementation of Principle 2 and to providing consumers with the control and transparency they desire. Moreover, data providers should be allowed to play a role in helping customers share only what data is necessary, such as by taking an active part in authorization, having access tokens expire after a set period, and providing dashboards where customers can monitor and manage their permissioned third parties. TCH further reiterates that sunsetting the practice of screen scraping is essential to achieving the limitation standard the Bureau has outlined.

B. Limits on Collection (Questions 89–90)

The Bureau notes that it is considering proposals to limit authorized third parties' collection of consumer information to what is reasonably necessary to provide the product or service the consumer has requested. The Bureau further proposed limiting the duration and frequency of information access and requiring that third parties provide consumers a simple way to revoke

[111] *Id.* at 40.

[112] *Id.* at 40–41.

[113] *Id.* at 41.

authorization.[114] The Bureau requests information on whether additional collection limitations are needed for potentially sensitive information that might cause particular harm to consumers if exposed, such as Social Security numbers. As noted by TCH on page 36 above, section 1033(a) of the Dodd-Frank Act does not mandate the provision of PII; instead, the obligation on a covered person is narrower—to provide "information in the control or possession of the covered person concerning the product or service the consumer obtained…."[115] Moreover, third parties can obtain that kind of information directly from the consumer. Given the heightened sensitivity associated with PII (other than information needed in certain use cases to confirm account ownership, such as name, address, email address, and telephone number), there are clear benefits to ensuring that consumers go through the exercise of providing this information directly to third parties rather than having their data providers pass it along.

The Bureau also asks whether third parties using screen scraping could comply with limits on collection. As discussed more fully on page 13 above, screen scraping, by its nature, gives access to the *entire* consumer account and results in the collection of more information than may be needed to provide the product or service requested. Consequently, the practice should be subject to a reasonable sunset established by the Bureau.

1. Duration and Frequency of Third-Party Access (Questions 91–93)

The Bureau notes that it is considering limiting authorized third parties to accessing consumer-authorized information for only as long and as often as would be reasonably necessary to provide the product or service the consumer has requested. [116] The Bureau further notes that it is considering limiting authorized duration to a maximum period, after which third parties would need to seek reauthorization for continued access.

TCH believes that the approach the Bureau is considering to limit duration and frequency is generally appropriate. TCH notes, however, that both duration and frequency are use-case dependent. The duration and frequency needed to provide data for a one-time mortgage application are markedly different from the duration and frequency needed to provide data for a personal wealth management application. The industry should be empowered, through FDX or some other appropriate standard-setting body, to set reasonable standards on duration and frequency by use case, subject to a regulatorily defined maximum. Further, as discussed on page 28 above, to ensure consumers continue to wish to provide their data, data providers should have the right to require reasonable periodic reauthorizations that work for them and their customers.

Additionally, data providers should also have the right to place reasonable time, place, and manner restrictions on third-party data access to protect customers and infrastructure. A self-imposed limitation on data recipients relating to how much and how often they access data might not always be sufficient to prevent their volumes or patterns of access from causing harm to data providers' systems. There is significant subjectivity to how much access a data recipient might think is "reasonably necessary" to provide the product or service to the customer, and the cumulative

[114] *Id.*

[115] 12 U.S.C. § 5533(a).

[116] SBREFA Outline, *supra* note 5, at 41.

effect could be that third-party data access could consume a majority of a data provider's infrastructure bandwidth if reasonable time, place, and manner restrictions are not established.

The Bureau requests input on how it could reduce negative impacts on consumers and unnecessary costs for authorized third parties if it were to adopt a rule to require third parties to obtain reauthorization after a durational period has lapsed.[117] The Bureau asks whether it should consider proposals that would allow authorized third parties to (1) seek reauthorization, either before authorization lapses, or within a grace period after authorization lapses; (2) establish a presumption of reauthorization subject to a consumer's ability to opt out of the presumption, based on the consumer's recent use of a product or service; or (3) require all authorized third parties to obtain reauthorization on the same day during the same month each year for all consumers.

TCH believes that reauthorization should be required before an authorization lapses to provide maximum consumer control and transparency and that there should be no grace period. Further, TCH believes that a presumption of reauthorization should not flow from a consumer's recent use of the product or service. A consumer may forget the parameters they established for data access and use and their use of a product or service may change over time. Reauthorization is an essential activity to ensure that data is being accessed in the scope that is most consistent with the consumer's current use of the product or service. TCH also believes that obtaining reauthorization on the same day and same month each year for all consumers is neither practical nor wise. Large data aggregators and other third parties may have to divide this task over many months for operational reasons. In addition, a once-a-year same-day, same-month reauthorization program may result in notices that lack meaningful context for the consumer. Last, TCH believes that whatever process is embodied in the rule must be able to be automated in order for the process to be scalable.

2. Revoking Third-Party Authorization (Questions 94–97)

The Bureau notes that it is considering requiring authorized third parties to provide consumers with a simple way to revoke authorization at any point, consistent with the consumers' mode of authorization. TCH believes that the ability to easily revoke consumer consent is fundamental to ensuring consumer control. It should be as easy for consumers to revoke authorization as it is to give it.

The Bureau requests input on whether covered data providers should also be required to provide consumers with a mechanism by which they may revoke third-party authorizations and whether it is feasible to require covered data providers to provide revocation mechanisms where screen scraping is used.[118] TCH believes that it is essential that data providers have the ability to provide consumers with a mechanism by which they may revoke third-party authorizations, such as by allowing data providers to enable customers to manage authorization permissions via the data provider's online portal. Consumers will necessarily look to their banks to protect them and their data, and banks should be empowered to do so. It should be noted, however, that it will not always be feasible for banks to easily provide a mechanism to revoke authorization where the third party is using credential-based access and screen scraping because the banks may not be able to distinguish between the consumer and the third party.

[117] *Id.* at 42.

[118] SBREFA Outline, *supra* note 5, at 42.

The Bureau requests input on whether authorized third parties should be required to report consumer revocation requests to covered data providers.[119] Revocation that takes place at the data provider is preferable in that the data provider can properly control access. If revocation takes place at the third party, then it will be important that such revocation be immediately transmitted to the data provider so that both the data provider and the third party are in sync.

The Bureau seeks information on how it should address consumers' potential desire to revoke access for certain, but not all, use cases.[120] It is unclear how the Bureau would define use case in this instance. If what is meant by use case is a data aggregator supplying data to two different data users and the ability to turn off one user, that should be feasible. If what is meant by use case is that a single entity accessing data for two different purposes and the consumer desires to turn off one, developing that capability would be substantially more difficult and costly. Current technology allows consumers to turn off data access by entity, not typically by use case. To limit cost and ensure feasible implementation, TCH recommends that the Bureau pursue a proposal that is in line with current technology.

3. Limits on Secondary Use of Consumer-Authorized Information (Questions 98–102)

The Bureau notes that it is considering proposals that would limit third parties' secondary use of consumer-authorized information. The Bureau would define secondary use to mean a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested, including the third party's own use of consumer data and the sharing of data with downstream parties. The Bureau notes that it is considering various approaches, including prohibiting (1) all secondary uses, (2) certain high-risk secondary uses, (3) any secondary uses unless the consumer opts into those uses, and (4) any secondary use if the consumer opts out of those uses.[121]

While all secondary uses carry some risk, insofar as the data is used for reasons other than providing the product or service that had motivated the consumer to share their data in the first place, some secondary uses are riskier than others. The use of de-identified data may be considered less risky in certain circumstances than alternatives, such as using PII for marketing purposes, however. Accordingly, TCH believes the Bureau should adopt a nuanced approach, with riskier secondary uses requiring affirmative consumer opt-in and less risky secondary uses requiring consumer opt-out. For clarity, however, TCH reiterates its stance that the Bureau should prohibit the sale of consumer data unrelated to the direct provision of any authorized product or service to the consumer.

4. Limits on Retention (Questions 103–110)

The Bureau is considering proposing that authorized third parties be obligated to limit their retention of consumer-authorized information. Specifically, the Bureau is considering requiring third parties to delete consumer information when it is no longer reasonably necessary to provide

[119] *Id.* at 43.

[120] *Id.*

[121] *Id.*

the consumer's requested product or service or when the consumer revokes their authorization.[122] The Bureau is also considering a limited exception to the deletion requirements for compliance with other laws.

TCH believes that the right to be forgotten is an important part of consumer control and transparency and is therefore supportive of a final tule that requires authorized third parties to delete consumer information that is no longer reasonably necessary to provide the requested product or service. Third parties should be permitted to retain consumer information beyond receipt of the consumer's revocation request only where required by law. Even then, third parties should be required to disclose to consumers that the authorized information is being retained. To protect consumers and the data-sharing ecosystem, there should be no circumstance sufficient to justify a third party's retention of consumer credentials. Further, deletion should also be required when authorization lapses at the end of a durational period unless there is timely reauthorization.

The Bureau requests information on what requirements should be imposed on authorized third parties that utilize screen scraping and potentially collect more information than what is reasonably necessary to provide the product or service.[123] TCH strongly believes, for the reasons discussed more fully on page 31 above, that the Bureau should sunset the practice of screen scraping. Until such time as screen scraping is abolished, third parties engaged in screen scraping should be required to delete information that is not reasonably necessary to provide consumers with the product or service.

The Bureau requests input on whether it should entertain more flexibility for third parties to retain certain information (besides an exception for compliance with other laws), such as de-identified consumer information.[124] Because the retention of consumer information is inherently risky and not necessary to provide the product or service, TCH believes that exceptions should be narrowly drawn and limited to compliance with other laws. The retention of de-identified data should be no exception to the general rule.

C. Data Security

The Bureau is considering a proposal to require authorized third parties to implement data security standards to prevent these third parties from exposing consumers to harms arising from inadequate data security. The Bureau is considering two alternative approaches. One option would be to require authorized third parties to develop, implement, and maintain a comprehensive written data security program appropriate for the third party's size and complexity and for the volume and sensitivity of the consumer information at issue. of the other option would require authorized third parties to comply with the Safeguards Rule or the Safeguards Guidelines.[125]

TCH is aware that some data aggregators have argued that they are not subject to the requirements of the Gramm–Leach–Bliley Act and its implementing regulations because they are

[122] SBREFA Outline, *supra* note 5, at 44.

[123] *Id.* at 45.

[124] *Id.*

[125] The Bureau uses "Safeguards Rule" to refer to the FTC's Safeguards Rule (16 C.F.R. pt. 314) and "Safeguards Guidelines" to refer to the guidelines adopted by the federal prudential regulators. *See* SBREFA Outline, *supra* note 5, at 45, n.49.

not "financial institutions" as defined in section 509(3)(A) of that statute.[126] It will therefore be important to ensure that all third parties are covered by data security requirements.

TCH notes that the Safeguards Guidelines are far more detailed than the Safeguards Rule and believes that the best way to prevent authorized third parties from exposing consumers to harms arising from inadequate data security and to ensure the consistent protection of data across the data-sharing ecosystem is to apply the Safeguards Guidelines to all participants in that ecosystem. In addition to applying the Safeguard Guidelines to all participants, those participants need to be subject to active supervision and enforcement if there is to be meaningful consumer protection.[127] Additionally, even with data security standards in place, the CFPB should ensure that third parties and data aggregators take liability for harm caused as a result of security breaches, security lapses, or data misuse.

D. Data Accuracy and Dispute Resolution

To ensure data accuracy and appropriate dispute resolution, the Bureau is considering a proposal to require authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the information they collect and use to provide the product or service the consumer has requested, including procedures related to addressing disputes raised by consumers.

TCH notes 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 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.[128] 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 and should rather be permitted to rely on their existing infrastructures.

Conversely, consumers generally face a much different environment in attempting to resolve issues with data aggregators and 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 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 hack at Robinhood Markets are illustrative.[129] Even in cases dealing with fraudulent transfers from Robinhood's accounts—circumstances that required an immediate and urgent response to prevent

[126] 15 U.S.C. § 6809(3).

[127] See discussion of supervision and enforcement on page 28.

[128] For example, FIs already have detailed regulatory requirements under EFTA and its implementing regulation, Regulation E, and TILA and its implementing regulation, Regulation Z, for resolving disputes relating to unauthorized transfers and unauthorized credit card charges. *See*, *e.g.,* 15 U.S.C. § 1693g(a)/12 C.F.R. § 1005.6(b) (limiting consumer liability for unauthorized electronic fund transfers); 15 U.S.C. § 1643(a)/12 C.F.R. § 1026.12(b)(1)(ii) (limiting cardholder liability for unauthorized charges to $50).

[129] Sophie Alexander & Anders Melin, *Robinhood User Says $300,000 Restored From Hack, Then Taken Back*, BLOOMBERG (Dec. 22, 2020).

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."[130]

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 providers will need to be a part of any regulatory framework that the Bureau adopts in implementing section 1033 of the Dodd-Frank Act. As with other requirements, to ensure meaningful compliance, any rule developed by the Bureau must be accompanied by appropriate supervision and enforcement.

E. Disclosures Related to Third-Party Obligations (Questions 117–118)

The Bureau is considering proposals related to disclosure requirements applicable to authorized third parties to enable consumers to make informed decisions, including requiring authorized third parties to periodically remind consumers how to revoke authorization and to provide consumers with a mechanism to request information about the extent and purpose of the authorized third parties' access.[131]

TCH believes third parties should provide a standing disclosure of how to revoke authorization that is clear and conspicuous. The ability to revoke authorization is fundamental to consumer control, and consumers should not have to hunt for the means to revoke authorization whenever they desire to do so. In addition, disclosures regarding the extent and purposes of the authorized third party's access to consumer data should also appear as part of a standing disclosure. The data being accessed and the use to which is put is an essential part of transparency; consumers need to have this information to make informed decisions whether to continue or to revoke their authorization.

X. Record Retention Obligations

The Bureau is considering proposing record retention requirements for covered data providers and authorized third parties for documents that would demonstrate their compliance with certain requirements of the rule. The Bureau requests information about the costs to covered data providers and authorized third parties that would be associated with such a requirement. The Bureau also requests input on whether covered data providers and authorized third parties should be required to maintain policies and procedures to comply with their obligations under the rule.[132]

TCH notes that information regarding costs is highly dependent on the specific records that would need to be maintained. Absent such detail, it is difficult, if not impossible, to provide meaningful information as to the associated costs. Regarding policies and procedures, TCH notes that banks are highly regulated and supervised and have sophisticated risk management frameworks in place. Accordingly, banks will likely maintain such policies and procedures regardless of any CFPB requirement. By contrast, third parties, are not regulated and supervised like banks and will not likely maintain such policies and procedures absent a specific requirement.

---

[130] *Id.*

[131] SBREFA Outline, *supra* note 5, at 47.

[132] *Id.* at 48.

XI. Implementation Period

The Bureau seeks input on an appropriate implementation period for complying with the final rule, other than potential third-party access portal requirements. TCH notes that, given the potential breadth of options the Bureau is considering and uncertainty as to the scope of the Bureau's ultimate proposed rulemaking it is difficult, if not impossible, to provide meaningful input on an appropriate implementation period. To the extent that the Bureau develops a final rule that is consistent with current industry practices for API-related data access, implementation could be comparatively swift, particularly if small institutions leverage the efficiencies provided by utilities like Akoya. To the extent the Bureau develops a final rule that materially departs from current industry practices or standards developed by industry standard-setting organizations like FDX for API-related data access, however, the implementation period would need to be comparatively—and substantially—longer.

XII. Potential Impacts on Small Entities

The Bureau seeks detailed information with which to estimate the potential impact of the rule on small entities, including the costs that those entities would incur to comply with the proposals.[133] While much of the information sought by the Bureau will have to come from individual institutions, TCH makes the following observations:

- To the extent the Bureau enlarges the scope of covered data providers to comply with the statutory mandate, the number of covered data providers that are small entities will be substantially enlarged.[134]
- The cost estimates outlined by the Bureau seem extremely low and not consistent with costs incurred by entities that have already enabled API access. The Bureau should engage with data providers that are currently providing API access to ensure real-world figures are being used to estimate costs.
- The scope of potentially covered data outlined in the proposals extends well beyond that which is currently provided in periodic statements and through account management portals (and as discussed more fully on pages 36–37 above, goes well beyond what the Dodd-Frank Act mandates data providers make available). Any delta between current market practices and the Bureau's requirements would substantially increase the costs of compliance.
- Smaller institutions may be able to leverage industry utilities like Akoya to realize efficiencies that will bring associated cost savings.[135]
- The Bureau's estimate of costs likely to be incurred in developing policies, procedures, and disclosures seems to contemplate only the legal resources needed for drafting. In reality, the creation of policies, procedures, and disclosures requires the involvement of cross-functional teams, with representatives from Product, Legal, Operations, Risk Management, and Compliance. As such, TCH believes that the Bureau's cost estimates related to the

[133] *Id.* at 49.

[134] See discussion of proposed definition of covered data provider on pages 23–25 above.

[135] See discussion of Akoya on page 18 above.

development of policies, procedures, and disclosures are significantly lower than what would actually be incurred.

XIII. Conclusion

TCH appreciates the opportunity to comment on the outline of proposals under consideration by the Bureau for its rulemaking on personal financial data rights under section 1033 of the Dodd-Frank Act. As discussed more fully above, TCH and its members are fully supportive of the right of consumers to safely and securely obtain information, upon request, about their ownership or use of a financial product or service from the provider of that product or service. To that end, TCH and its members have committed substantial time, effort, and resources to ensuring that the financial services ecosystem supports that right. TCH hopes that as the Bureau moves forward with its rulemaking it will seek ways to ensure that the final rule is minimally disruptive of and does not diminish the substantial progress that has already been made by the private sector in creating an infrastructure that facilitates safe, secure data sharing consistent with the Bureau's previously issued guidance. TCH looks forward to further engagement with the Bureau as the rulemaking process unfolds.

Sincerely,

/s/ Robert C. Hunter

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