
January 25, 2023

*Via electronic submission*
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552
Attn: Comment Intake

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

To Whom It May Concern:

The Bank Policy Institute[1] appreciates the opportunity to comment on the Outline of Proposals and Alternatives Under Consideration regarding the required rulemaking on personal financial data rights[2] issued by the Consumer Financial Protection Bureau pursuant to Section 1033 of the Dodd-Frank Act.[3] The CFPB previously has stated and reiterates in the Outline that "[d]ata access rights . . . hold the potential to intensify competition in consumer finance . . . in three main ways: by enabling improvements to existing products and services, by fostering competition for existing products and services, and by enabling the development of new types of products and services.[4] BPI supports

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's bank-originated small business loans, and are an engine for financial innovation and economic growth.

[2] Consumer Financial Protection Bureau Small Business Advisory Review Panel for Required Rulemaking On Personal Financial Data Rights: Outline of Proposals and Alternatives Under Consideration (Oct. 27, 2022), available at: Small Business Advisory Review Panel for Consumer-Permissioned Sharing of Consumer Financial Data Rulemaking Outline of Proposals and Alternatives Under Consideration (consumerfinance.gov).

[3] 12 U.S.C. § 5533.

[4] Outline at 4, *citing* Bureau of Consumer Fin. Prot., Advance Notice of Proposed Rulemaking, Consumer Access to Financial Records, 85 FR 71003 (Nov. 6, 2020). In considering its implementation of section 1033 of the Dodd-Frank Act, the CFPB has taken the view that it must implement rules that would broadly require data providers to provide a vast trove of consumers' information to certain third parties – data users and data aggregators

innovation and welcomes competition in financial products and services, so long as the innovation is conducted responsibly, consumers' data is protected, and all entities operating in the ecosystem are subject to consistent regulation and examination.

The growth in adoption of digital products and services in recent years has accelerated banks' efforts to leverage market-developed technological solutions to help meet customer demand while ensuring consumers' sensitive financial data is kept private and secure.[5] Unlike other jurisdictions in which consumer financial data sharing has been mandated by government action, this expansion of consumer financial data access in the United States largely has developed via innovation in the marketplace. Under an industry-driven approach, participants can innovate and adapt more quickly to meet consumer demand and develop safer solutions.

In the United States, as consumer demand for more digital and interactive financial products and services has increased, an increasing number of financial technology firms ("fintechs") and other companies not subject to the same comprehensive regulatory oversight as banks have entered the market for consumer financial products and services. These entities, in turn, increasingly have sought permission from consumers to access their sensitive consumer data held at a financial institution to provide such products and services.[6] We support the ability of bank customers to securely connect their bank accounts to the third-party apps of their choice, which can involve the use of a data aggregator to retrieve the customer's information from the customer's financial institution and share it with the app. It is critical, however, that consumers' personal and financial information remains secure when it is shared between financial institutions and third parties.

---

(designated as "authorized third parties" in the CFPB's Outline) – based on the consumer's authorization obtained by a third party. We note that the language of section 1033 provides only that covered persons shall make available to a consumer "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." Within the larger context of the CFPA, "consumer" is defined as "an individual or an agent, trustee, or representative acting on behalf of an individual," although the CFPB itself did not always assume that third parties such as data users and data aggregators would be included within the scope of an "agent, trustee, or representative" of a consumer, as reflected in the CRPB's ANPR in which it asked for input on the question of: "Who should be considered 'an agent, trustee, or representative' of an individual consumer for purposes of implementing section 1033 access rights? Should any exclusions apply? If so, what exclusions and why? Or even if a data user whose product a customer wants may be considered an 'agent,' what about data aggregators who are relied upon by agent firms but frequently lack a relationship with customers themselves?" *See* CFPB, "Consumer Access to Financial Records," Advance notice of proposed rulemaking 85 FR 71003 (Nov. 6, 2020) 71003, 71010, *available at*: 2020-23723.pdf (govinfo.gov).

[5] The increased shift towards digital financial products and services has been driven in part by the COVID-19 pandemic. *See*, *e.g.*, American Bankers Association, "National Survey: Bank Customers Turn to Mobile Apps More Than Any Other Channel to Manage Their Accounts: COVID-19 accelerated move toward digital banking channels" (Oct. 25, 2021), available at: National Survey: Bank Customers Turn to Mobile Apps More Than Any Other Channel to Manage Their Accounts | American Bankers Association (aba.com).

[6] *See* U.S. Department of the Treasury Report to the White House Competition Council "Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets" (Nov. 2022), available at: Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets (treasury.gov).

The CFPB has engaged in various information gathering efforts in preparing to propose a rule to implement section 1033 of the Dodd-Frank Act, including issuing a Request for Information Regarding Consumer Access to Financial Information,[7] establishing the *Principles for Consumer Authorized Financial Data Sharing and Aggregation* (Principles), published in October of 2017,[8] and issuing an Advance Notice of Proposed Rulemaking.[9] The Outline represents the latest step by the CFPB to promulgate rules under section 1033 and seeks input from small business entities to help the CFPB assess the impact on those entities by the proposals under consideration, as required by the Paperwork Reduction Act. Throughout the Outline, the CFPB poses questions for small business entities, and the CFPB also has invited "feedback from data providers and third parties that access data on behalf of consumers."[10] BPI members are not small entities, but have a significant interest in the Proposals Under Consideration set forth in the Outline, primarily as data providers, but also as third parties that may be authorized by their customers to collect customer-authorized information from other data providers. BPI appreciates the opportunity to provide input on the Outline from those perspectives.

We make several observations and recommendations regarding the Outline, as described in greater detail below.

## I. Introduction.

Although this letter addresses the details of many specific aspects of the proposals in the CFPB's SBREFA outline, any final rule should be principles-based rather than overly technical and prescriptive in order to accommodate quickly evolving advancements in the market. The CFPB should implement a rule that builds on its own 2017 Principles, as this is the framework on which the industry has relied to innovate to provide consumers access to a broader range of financial products and services. A principles-based approach also will allow for flexibility and incremental changes within the ecosystem that will be necessary as the marketplace continues to evolve. Most critically, rulemaking should codify the most important CFPB principles: (1) consumers must have transparency into and control over where, how, and the extent to which their data is shared;[11] (2) information must be secure and protected with bank-like security no matter where it resides;[12] and (3) entities that cause either direct or indirect harm to consumers are responsible for remedying the harm.[13] Any final rule should allow participants in the

[7] 81 FR 83806 (Nov. 22, 2016).

[8] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf (accessed Jan. 23, 2023)).

[9] Bureau of Consumer Fin. Prot., Advance Notice of Proposed Rulemaking, Consumer Access to Financial Records, 85 Fed. Reg. 71003 (Nov. 6, 2020).

[10] Outline at 8.

[11] CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Principles 3 and 6.

[12] CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Principle 5.

[13] CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Principles 8 and 9.

ecosystem the flexibility to develop and amend their specific practices to facilitate data sharing consistent with the key principles of consumer transparency and control, data security, and fair liability apportionment.

The success of industry-led initiatives, such as widely adopted API standards through the Financial Data Exchange (FDX) and achieving one-to-many connectivity through Akoya,[14] a central utility, underscores the ability of market participants to self-regulate and develop best-in-class, market leading standards and practices for data sharing and aggregation. Any final rule should not deter or detract from these initiatives and efforts and should allow participants in the ecosystem the flexibility to develop and amend their specific practices to facilitate data sharing consistent with the key principles of consumer transparency and control, data security, and fair liability apportionment.

Overly prescriptive rules would slow progress and could potentially undo the important consumer protections that have been developed in connection with industry-led efforts. Thus, while this letter offers detailed responses to several issues raised by the CFPB's Outline, the CFPB should establish a high-level framework consistent with the key principles the CFPB has identified within which market participants can establish standards and requirements that reflect the technological and operational realities of data sharing and adjust those over time as technological changes occur and consumer demand shifts. This approach would appropriately allow for innovation and development in consumer protections in a manner reflecting the speed with which changes occur in this ecosystem.

A principles-based approach also would allow the market to continue to evolve and answer some of the questions the CFPB poses in the Outline, such as questions related to the level of detail that is optimal for consumers in granting a third-party authorization to collect the consumer's information. An overly prescriptive approach, by contrast, as contemplated in the Outline would, in some ways, go beyond what the statute authorizes and could undermine the progress that has been made to date in the consumer information sharing ecosystem. Increasing consumer-authorized data sharing with no clear consumer benefit could unnecessarily put consumers' data at risk for theft and misuse. This overly prescriptive and sweeping approach appears to derive, at least in part, from the CFPB's underestimation of the robust competition that exists in the consumer financial services marketplace today, driven in part by the robust data sharing ecosystem that has developed in the market. Consumers in the U.S. currently benefit from a unique financial services market that is significantly more competitive than any other jurisdiction in the world, including those where "Open Banking" regulations have been implemented.[15]

---

[14] Akoya provides "a single integration" through which "financial institutions, fintechs, and data aggregators can enable multiple API connections" and "avoid continued maintenance and development efforts." *See* https://akoya.com/about.

[15] For example, PSD2 was implemented in the EU/UK in 2019 and requires financial institutions to share consumer data with third party payment service providers with the goal of increasing competition in consumer financial services. Yet, despite the implementation of these standards, seven banks in the UK maintain approximately 93 percent market share, while in the EU, there are only approximately 5,400 financial institutions across all 27 EU members combined. *See* Reuters Graphics, "Britain's banks by market share," available at: http://fingfx.thomsonreuters.com/gfx/editorcharts/VIRGIN%20MONEY-M-A-CYBG/0H0012Y5G10G/index.html; *see also* Eurostat. Number of banks decreasing. There are nearly 10,000 financial institutions in the United States, including more than 4,300 FDIC-insured banks and nearly 5,300 credit unions. *See* Statista, Number of FDIC-insured

If many of the CFPB proposals are adopted as set forth in the Outline, this rulemaking could further entrench the concentrated position of dominant data aggregators and big tech companies, legitimizing the aggregation of consumer data at massive scale. Because of the critical importance of protecting the safety and security of consumer information, the CFPB should subject authorized third parties, such as data aggregators and data users, to data privacy and data security requirements and to direct supervision and examination for compliance with those requirements to help ensure that consumer data is protected, as previously suggested by industry participants.[16] Supervision, examination and enforcement of these third parties would ensure accountability and require corrective action by third parties in the event the standards and requirements were not met, which would incentivize all parties in the ecosystem to strengthen their safeguards for consumer personal financial data, to the benefit of consumers.[17]

---

commercial banks in the United States from 2000-2001 and Number of credit unions in the United States from 2013 to 1st half 2022. When compared to peer essential industries in the U.S., market share in banking is significantly less concentrated than in industries such as air transportation, telecommunications, motor vehicle manufacturing, grocery stores, and home furniture stores. *See* BPI/MBCA Joint Letter re: Enforcement policy respecting bank mergers at 14-15. In addition to regulated financial institutions, consumers in the U.S. currently have ready access to a wide range of non-bank financial products and services that, in many cases, directly compete with traditional financial products and services. As of November 2021, there were more than 10,700 registered fintech startups in the Americas alone, the highest number globally. By comparison, there were 9,300 such startups in Europe, the Middle East, and Africa combined; and 6,300 in the Asia Pacific region. *See* Statistica, Number of fintech startups worldwide from 2018 to 2021, by region. As noted in a recent Treasury report, there has been a substantial growth in the number of non-bank firms entering the market, offering consumers many of the same products and services offered by insured depository institutions. *See* US Treasury Report to the White House Competition Council, Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets at 11. According to Plaid, a large data aggregator, eight in ten consumers use some type of digital financial tool, with the average consumer using over three such tools. *See* Plaid, 2022 Fintech Report: The Fintech Effect - Stability, impact, and building for the future.

[16] *See* US Treasury Report to the White House Competition Council, Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets, 87-88 ("...there is virtually no regulatory oversight of data aggregators' storage of consumer financial information akin to the supervision of [banks'] data security)." *See also "*Petition to The Consumer Financial Protection Bureau for rulemaking defining larger participants of the aggregation services market," American Bankers Association, Consumer Bankers Association, Credit Union National Association, Housing Policy Council, Independent Community Bankers of America, National Association of Federally-Insured Credit Unions, National Bankers Association, and The Clearing House Association (August 2, 2022), available at: Regulations.gov; *see also* BPI comment letter in support of the joint trades petition for rulemaking defining larger participants of the aggregation services market (Oct. 3, 2022), available at: BPI-CFPBcommentreDataAggregatorPetitionforRulemaking-2022.10.03.pdf.

[17] Some third parties have been required to modify their privacy and data security practices via private class action settlements, which has included providing clearer disclosures regarding their use of data, deleting data for which there no longer is a valid account or means by which to authenticate the consumer, and minimizing future collection of data. Resolving data security and privacy considerations via class actions, however, has limited reach; instead, direct regulation of Third Parties by the CFPB would ensure a more efficient and consistent approach in regulating the privacy and security practices of these Third Parties to the benefit of consumers. In addition, direct regulation and supervision would help ensure that third parties' privacy and data security practices meet the relevant requirements and expectations before consumer harm has occurred rather than after such harm may have already occurred.

The CFPB also should establish a liability framework under which the entity with possession, custody, or control over the data or which is otherwise responsible for consumer loss or harm will be liable for the loss or harm. For data providers, any liability for any incident leading to loss or harm should end when the data leaves the data provider's portal.

We elaborate further below on these points and make the following recommendations that the CFPB should consider incorporating into any future proposed rule:

- **The CFPB should establish a date certain to ban screen scraping.**

- **The CFPB should revise certain aspects of its proposed authorization framework.**
  - Data providers should have flexibility regarding the authorization process.
  - Data providers should be able to reject a third party's request for a customer's data if certain conditions are not met.
  - Consumers must have transparency into and control over the terms under which their data would be shared.
  - Data providers should be permitted to impose reasonable time, place, and manner restrictions on data access.

- **Third parties should be subject to CFPB supervision and examination**.

- **The CFPB should establish a framework that fairly apportions liability among data providers and third parties**.

- **Data providers should have flexibility to determine what information to share with third parties**.

- **The CFPB should prohibit reverse engineering of confidential commercial information**.

- **Banks should not be required to share customer information in a manner that conflicts with their obligations to operate in a safe and sound manner and protect consumer data**.

- **The CFPB lacks authority to impose data accuracy or recordkeeping requirements**.

- **The CFPB should provide a more accurate estimate of the costs data providers would incur under the proposal**.

## II. The CFPB should establish a date certain to ban screen scraping.

The banking industry has been working for years to develop technical solutions that enable consumer access to financial data while providing adequate data protections. To assist the CFPB in understanding the current environment, we highlight below recent technological innovations that demonstrate how the industry has improved the data sharing marketplace to better serve consumers.

The industry continues to move away from screen scraping and credential-based data access towards data sharing through an Application Programming Interface ("API"). An API facilitates the transfer of consumer financial data through tokenized access, thus removing credential sharing and allowing users to be securely authenticated at their own financial institution. Data sharing through APIs is more accurate and secure than screen scraping and credential-based data access, and continued adoption of APIs will benefit consumers and all market participants.

The financial services industry has collectively advanced the marketplace towards common technical standards for the secure access of consumer-permissioned data. For example, through FDX, a cross-section of banks, third-party fintechs, data aggregators, consumer groups, and other financial industry groups have aligned around a common API to standardize the security and authentication for data transfer.[18] As a result of the development of the FDX API and the efforts of banks to make consumer data available via API, over 42 million U.S. consumers have already been transitioned away from screen scraping to a version of the FDX API.[19] The CFPB's efforts to implement Section 1033 of the Dodd-Frank Act should not reverse the significant progress that the industry has made or slow the pace of continued evolution in this space, which has generally benefited consumers.

Despite the industry's progress, screen scraping remains a widely used method for accessing not only payments account data, but also other types of data that are less accessible through a bank account (such as payroll data), thus enabling data harvesting of credentials to continue. The CFPB should set a deadline to sunset the practice of credential-based access, such as screen scraping, which would help accelerate the migration of consumer data sharing to APIs. Screen scraping through the use of a token presents fewer risks, but should still be eliminated, as it does not allow consumers to control the data shared with third parties. The technology exists today to migrate to APIs, but market participants may never have the incentive to transition to APIs if screen scraping is allowed to continue, including if it is retained in some form as a fallback mechanism. The migration of thousands of banks, data aggregators and fintechs to APIs in the United States for sharing consumer data would be a significant undertaking, particularly for those banks that may not have actively participated in the market-driven movement towards APIs that has occurred to date. Indeed, this process could take several years to complete. For this reason, it is critical to establish a specific timeline *now* to end screen scraping so that all market participants begin to work towards a future ecosystem where all consumers are able to share their information on an informed basis and in a safe and secure manner. Moreover, API solutions that are offered through a service provider would allow for a more cost effective and time effective transition to API-based access, and the CFPB should take steps to allow for this more broadly.

The CFPB's outline states that it is considering proposing that covered data providers would be required to establish and maintain a third-party portal that does not require the authorized third party to possess or retain consumer credentials. We agree that screen scraping and credential-based access should be prohibited at a certain future date for the following reasons.

First, screen scraping, whether using account credentials or a token, does not allow consumers

[18] *See* Financial Data Exchange website at https://financialdataexchange.org/.

[19] *See* FDX Press Release: "Financial Data Exchange (FDX) Reports 42 Million Consumer Accounts on FDX API" (Oct. 31, 2022).

or data providers to control the amount of data they share with third parties, and there is no way to ensure that the information "scraped" and maintained by the aggregator does not go beyond what is necessary for the third-party financial app to deliver the services sought by the consumer or what was specifically authorized by the consumer. Additionally, there is the risk that the aggregator or third-party app may continue to collect and store the consumer's data and credentials even after the consumer ceases using the financial app or revokes account access authorization. Several large data aggregators have engaged in this practice and have been required to delete consumer personal financial data that the consumer did not ask the data aggregator to collect but that they retrieved and stored anyway.[20]

Second, credential-based screen scraping creates opportunities for malicious actors to gain access to a consumer's accounts at a financial institution and commit fraud, or even take over the consumer's account. As former FinCEN Director Kenneth A. Blanco has previously warned, "[i]n some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires. By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms' integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts."[21]

Third, screen scraping can divert the cybersecurity resources of regulated financial institutions away from preventing truly unauthorized access by criminals or other bad actors, because in many cases, it is difficult for a financial institution to distinguish "legitimate" data aggregator logins from illegitimate traffic. This problem is compounded by the fact that some data aggregators bypass security controls used by financial institutions to authenticate customer logins (such as by auto-populating the security questions posed when a new connection is sought to be established with a consumer's account). As the Basel Committee on Banking Supervision found in its 2019 "Report on open banking and application programming interfaces," "[s]creen scraping or reverse engineering can undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the

---

[20] For example, in July 2022, a federal judge approved a $58 million settlement of certain data collection and use claims against Plaid, Inc., which provides login services for banking applications, and linking and verification services for various financial technology applications. Plaid also agreed to certain changes to its data collection practices, including: deleting data from its systems that was retrieved as part of Plaid's "Transactions" product for users that Plaid can reasonably determine did not connect an account to an application that requested Transactions data; deleting data from its systems for users for whom Plaid is aware that it no longer has valid means that can be used to authenticate with the financial institution; including a prominent reference to Plaid Portal on its website homepage along with a link to the Plaid Portal and a plain-language description of the user controls available; ensuring that its standard Plaid Link flow includes certain disclosures; minimizing the data Plaid stores from users' financial accounts; and enhancing its End User Privacy Policy to provide more detailed information about Plaid's data collection, storage, use, sharing, and deletion practices. Plaid denied the allegations of privacy violations and the settlement agreement does not include any admission of wrongdoing by the company. *Cottle v. Plaid Inc.*, 20-cv-03056-DMR (N.D. Cal. Jul. 20, 2022), available at: Cottle v. Plaid Inc., 20-cv-03056-DMR | Casetext Search + Citator.

[21] Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Federal Identity (FedID) Forum and Exposition, *"Identity Attack Surface and a Key to Countering Illicit Finance"*, (September 24, 2019), *available at* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid.

customer, data aggregator, and an unauthorised third party that is logging in and extracting sensitive data."[22]

Fourth, screen scraping cannot provide consumers the same level of control over data sharing that APIs can. When an aggregator or third party accesses a data provider via screen scraping, the data provider has little to no visibility into the entity accessing the account. Indeed, it looks much like a consumer accessing the account themselves. Data providers are unable to: (i) tell who is accessing the data (e.g., the aggregator and/or associated data recipient), (ii) tailor the data that will be shared based on the use case, or (iii) offer a data sharing dashboard that gives consumers a place to view and control what entities have access to their data.

The CFPB should not allow screen scraping as a back-up method of access during periods of API downtime. Doing so could cause consumer harm in several ways, including:

- By compromising the security of customers' sensitive information;
- By causing high volatility in traffic to banks' websites that could lead to outages impacting both third-party and "human" traffic;
- By causing customer confusion, as the consumer would have to both authorize API access with the data provider and separately provide their credentials to the third party; and
- Disregarding the customer's authorization, such as when a consumer has granted a third party only narrow access to certain data via a bank's API. If a third party were able to *also* screen-scrape, the third party would have unlimited access to data outside the scope, duration, and frequency that the customer has authorized, and neither the consumer nor the data provider would know what data had been accessed.

Europe's Payment Services Directive's Regulatory Technical Standards bans traditional screen scraping but requires financial institutions to implement a fallback mechanism in the event the API interface doesn't function properly.[23] The European rules require financial institutions to use contingency measures for API interfaces that experience "unplanned unavailability" or a "systems breakdown" which are presumed when five consecutive requests for access to consumer financial information have failed or not replied to within 30 seconds.[24] This has resulted in financial institutions developing both a traditional API interface and a fallback interface that still relies on the use of consumer authentication credentials, in some cases augmented by identification and authentication of the third party data recipients. In June 2022, the European Banking Authority published an opinion on its technical advice in connection with its review of the second Payment Services Directive ("PSD2") which explicitly recommended removing the fallback mechanism as an option. The European Banking Authority noted that such removal would create better incentives for parties to use APIs and concentrate their efforts on providing high-quality APIs, support the innovation and competition-enhancing objectives of PSD2, enhance security by enabling safe access to customer payment account

[22] Basel Committee on Banking Supervision, "Report on open banking and application programming interfaces (November 2019), *available at*: Report on open banking and application programming interfaces (APIs) (bis.org).

[23] *See* Europe's Payment Services Directive's Regulatory Technical Standards, Article 33 available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN.

[24] *See* Europe's Payment Services Directive's Regulatory Technical Standards, Articles 31-33.

data; and contribute to a level playing field across the EU.[25] The CFPB has articulated its goal of furthering many of those objectives in implementing section 1033, and the CFPB would be better able to achieve those goals by banning screen scraping as a fallback mechanism in any future rulemaking.

Prior to the date by which screen scraping would be banned, there should be a prohibition on third parties attempting to screen-scrape any data provider that makes data available via an API; and, if a data provider offers access via an API, that data provider should be permitted to block all screen-scraping by third parties. Without such a prohibition, it would be very costly for banks to effectively block screen-scraping, protect customers, and enforce usage of safer APIs. It can be complicated and expensive for data providers to monitor screen-scraping and effectively block it. Today, many financial institutions lack the tools to detect when third parties are "scraping" data and in what volumes. Even among large banks that do have such capabilities, it is expensive to block unwanted automated web scraping without also inadvertently blocking real "human traffic," especially if the third party repeatedly modifies their automated scripts to "look human" in an attempt to evade data providers' monitoring and blocking systems (as is common practice today among some third parties).

The CFPB's proposal that would allow third parties to screen scrape using tokens provided by data providers would undermine many of the important objectives that the CFPB has laid out in the Outline. APIs allow data providers to enable data access for third parties on the terms of access specifically authorized by the consumer, including terms related to scope, duration, and frequency. The approach of "using a token to screen-scrape" would enable access beyond the terms of what the consumer has authorized and fails to address many of the important risks associated with screen-scraping, such as third parties being able to make unauthorized payments on the customer's behalf or access proprietary data that banks are not obligated to share.

While traffic via APIs can in some respects be more efficient and less resource-intensive than screen-scraping, this is not universally true or a reason to allow unfettered API access. Requiring or promoting account mirroring (e.g., a third-party pulling data from a data provider every hour or seeking real-time updates) would impose a very high burden on data providers and overwhelm technology systems. A large share of aggregation use cases can be supported by one data pull per day, or even less frequent data pulls. Unfettered third party access to an API would introduce undue and excessive burdens on data providers, potentially requiring data providers to incur large costs to support much higher volumes of traffic, which has occurred in the ecosystem. Enabling API access requires separate technology services to be built and maintained and back-end systems are required to support the traffic. In addition, unfettered third party API access could harm customers by causing degradation of access on other channels, such as the data provider's website or mobile app. Therefore, as set forth below, reasonable time, place, and manner restrictions on third parties' ability to access consumers' sensitive

[25] *See* Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2, § 17.2, *available at* https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf.

financial information are necessary to protect not only consumers, but also the data ecosystem as a whole.

## III. The CFPB should expand the scope of covered data providers and products.

The CFPB states in the Outline that it is considering limiting the universe of data providers to entities that meet the definition of "financial institution" in Regulation E or "card issuer" in Regulation Z, which likely would limit data providers primarily to depository institutions and potentially a few fintechs that offer an "account" and electronic funds transfer services or that issue credit cards that relate to an open-end consumer credit plan.[26] Thus, data would largely flow from depository institutions to fintechs and other nonbank entities, while depository institutions would not be able to collect consumer-authorized information from those nonbanks to provide products or services to their customers requiring customer information held by those entities.

To realize the full benefits of the statute, consumers should have access to their data held by all entities offering a consumer financial product or service. Section 1033 provides that consumers may request certain information from "any entity that offers a consumer financial product or service;" thus, all such entities should be "covered entities" for purposes of the rule. To promote competition and benefit consumers, the CFPB should ensure data provider obligations apply not only to depository institutions and card issuers, but also companies providing investment or securities services, mortgages, digital wallets, other types of loans (e.g., BNPL), crypto, and all other entities that offer a consumer financial product or service as defined in the Dodd-Frank Act. Today, millions of consumers share their investment and mortgage account data with third parties, enabling these consumers to have a more holistic view of their finances and to seek various financial products and services offered by banks, fintechs and other entities. If the CFPB excludes these account types from section 1033, consumers may not realize the full benefits of the statute. For example, without access to information from all providers of consumer financial products and services, consumers may not be able to use personal budgeting apps, which may frustrate consumers' expectations with respect to accessing their personal financial data.

## IV. The CFPB should revise certain aspects of its proposed authorization framework.

The Outline provides that the CFPB is considering proposals related to authorization procedures for third parties to access consumer information on consumers' behalf that "seek to ensure that such third parties are acting on behalf of the consumer."[27] The proposals under consideration 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

[26] 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" 12 C.F.R. part 1005). Regulation Z defines "card issuer" as a "person that issues a card or that person's agent with respect to the card." 12 C.F.R. part 1026.

[27] Outline at 15.

obligations regarding collection, use, and retention of the consumer's information (certification statement)."[28]

The proposal further provides that "an authorization disclosure would contain key scope and use terms that may 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. Key use terms 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."[29]

Authorization disclosures should contain disclosures that are sufficiently clear and easily understood by consumers to ensure that authorization is knowingly given.

The CFPB has previously addressed consumer consent and authorization in "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." Principle 3 describes the critical elements of consumer consent and authorization:

> *Principle 3 – Control and Informed Consent. Consumers can enhance their financial lives when they control information regarding their accounts or use of financial services. Authorized terms of access, storage, use, and disposal are fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer. Terms of data access include access frequency, data scope, and retention period. Consumers are not coerced into granting third-party access. Consumers 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.*[30]

The CFPB has asked for comments on several aspects of its authorization procedures under consideration. As an initial matter, the Bureau has asked whether third party disclosure obligations should apply to the data recipient, the data aggregator, or both. To ensure that consumers are provided with all relevant information regarding what entities will have access to their data and under what terms, both the data aggregator and the data recipient should be required to provide disclosures to consumers, and these disclosures should be consistent with the CFPB's Principle 3.

Data aggregators and data recipients should be required to disclose to consumers the identity of each data recipient to which the consumer's data is being provided, and the consumer should have to provide authorization for each data recipient with whom information is shared. Consistent with Principle 3, disclosures should be required to include a clear and specific description of the data that is being

---

[28] Outline at 15 (emphasis added).

[29] Outline at 16.

[30] CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Principle 3.

accessed, how frequently it is being accessed, for what purpose, and for how long it is being stored. Disclosures must be sufficiently detailed, segregated from any other consumer agreement requests, and clear to be easily understood by consumers to help ensure that authorization is knowingly given. Data providers should have the ability to require periodic affirmative reauthorization from their customers. Reauthorization may reduce the ability of data aggregators or data recipients to continue to collect and store the consumer's data by forcing those entities to obtain consent periodically, thereby enabling the consumer to gain greater autonomy with respect to which parties may access their personal financial data and other important terms on which the data may be shared.

In addition, consistent with the CFPB's Principle 3, authorization disclosures should clearly spell out the consumer's right to revoke authorization and should include the right to request that their data be deleted by the third party, although data subject to GLBA or required to be retained for other legal or regulatory purposes should be exempt from the deletion requirement. The process for revoking authorization and/or deleting previously acquired data should be no more complex or onerous than the process associated with providing the original authorization and should be available via similar channels.

The Outline also states that the CFPB is considering proposals that would limit third parties' secondary use of consumer-authorized information, which the CFPB is considering defining as "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 entities."[31]

Under the Gramm-Leach-Bliley Act, reuse and redisclosure limitations are placed on downstream recipients of data that limit the ability of those downstream recipients to use or disclose the data for purposes other than those to carry out the activity under which the downstream recipients received the data.[32] Entities that are covered by GLBA may use data for secondary uses to which the consumer consents, and non-GLBA-covered entities may not. These restrictions (and process protections) would "travel" with the data. As discussed throughout this letter, the CFPB should apply the requirements of the GLBA to third parties and subject to them to direct, consistent oversight to ensure that they comply with the requirements of the statute. This is consistent with the principle of allowing customers to have control over the use of their data, and any proposed secondary use should be subject to clear disclosure and consumer authorization.

Secondary use may include the sale of consumer-authorized information. Data is generally sold in one of two forms: the raw data itself may be sold, or data that has been aggregated and anonymized and used to derive insights or conclusions may be sold. The CFPB should ban the sale of the former for any purpose, as the risk to consumers from the sale of raw data is high, and there does not appear to be a clear consumer benefit from selling their raw data.

The sale of aggregated and anonymized data should be permitted only if the customer is provided clear and conspicuous disclosure and has consented to the sale, and third parties should have

[31] Outline at 43.

[32] 12 C.F.R. 1016.11.

the flexibility to require the customer to affirmatively opt-in to such sale.[33] If reauthorization is required by a data provider, the data provider may require reauthorization for the secondary use cases to which the consumer has consented, including the sale of aggregated and anonymized data. The CFPB also should consider prohibiting third parties from re-identifying the aggregated/anonymized data.

Below, we provide additional recommendations regarding the authorization process.

**a. Data providers should have flexibility regarding the authorization process.**

The CFPB is considering requiring *third parties* to obtain customer authorization in writing or electronic form, evidenced by the consumer's signature or the electronic equivalent, and 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.[34]

We have concerns about requiring the authorization process to be conducted by a third party rather than by the data provider. The data provider has a preexisting relationship with the consumer, is a trusted and known entity to the consumer, and has an interest in protecting its customer's data. Data providers thus may be more likely to help ensure that the consumer maintains control over the sharing of her data and that the principle of data minimization is respected. Data providers also may provide dashboards where customers can directly monitor and easily manage their permissioned third parties. Allowing consumers to manage all aspects of their accounts, including data sharing of account-related information, directly with the data provider will allow consumers to more easily manage these accounts and control the extent to which they share their data and on what terms.

If the authorization process is not completed with a data provider, accountholders of accounts with one or more owners may not have visibility into connections made by a fellow accountholder, as the third party would not necessarily know about the specific relationships of accountholders to the account. A data provider likely would have to confirm any authorization provided by a third party with a customer, particularly when an account has multiple accountholders, as data sharing in such a scenario could run afoul of specific rights or terms and conditions agreed to among the accountholders. Because one of the fundamental principles of consumer data sharing is that consumers should have visibility into and control over whether, how, when, and with whom their data is shared, all accountholders on joint or multi-person accounts should have visibility and control over sharing account information with third parties, which is best achieved when the data provider controls the authorization process for all account holders and with respect to all third parties granted authorization to account information.

For these reasons, data providers should not be required to provide customer information to a third party based on authorization obtained by that third party, although data providers should have the flexibility to rely on authorizations obtained by a third party if they choose.

Third party control over the authorization process does not reflect how authorization occurs

[33] The regulations implementing GLBA provide a definition of "clear and conspicuous" that could provide a useful model for the CFPB in defining this term. 12 CFR 1016.3(b).

[34] Outline at 15.

through APIs today; generally, including under the FDX standard, a consumer is redirected by a third party to the data provider for authorization. As explained previously, this approach more effectively allows the consumer to maintain control, preserves the safety and soundness of the ecosystem, and prevents fraud, all of which significantly benefits consumers. FDX also has issued detailed user experience guidelines for the implementation of consumer dashboards at data providers and third parties and has developed tools to standardize user consent. The FDX standard aligns with and facilitates globally interoperable standards that are necessary for the expansion of the financial data sharing ecosystem and consistent with Section 1033's requirement that the CFPB should "take into account conditions under which covered persons do business both in the United States and in other countries." Were the CFPB to promulgate rules that did not conform with existing standards already in use to facilitate data sharing, there would be substantial and unnecessary burden and costs imposed on the industry to reestablish these standards, which would also delay the expansion of the safe and secure consumer financial data sharing ecosystem.

The CFPB should allow flexibility for data providers as to how they capture and honor the customer's scope of authorization through their online systems or portals/APIs. The CFPB should provide market participants with flexibility to build third-party data sharing solutions that honor the customer's scope of authorization. It would be extremely costly to create an API-based data-sharing ecosystem based on the authorization model proposed by the CFPB, where the authorization (including scope of data, duration, and frequency) is defined and captured by the data recipient instead of the data provider. When data providers create APIs, they generally must configure the scope of available data that can be retrieved by authorized third parties. In the CFPB's proposed model, the scope of authorization would be defined and captured not by the data provider, but by the data recipient. As noted, data providers should not be required to honor those authorizations; however, if they choose to do so, because there are many different data recipients, authorization could take on hundreds or thousands of different custom permutations. This would be like requiring every restaurant in America to allow customers to walk in and order any dish they want, composed of any imaginable ingredient, regardless of the menu, and, in cases where the customer's order was ambiguous, establish a process for clarifying what they meant, all while continuing to provide regular service to millions of customers every day. This would be enormously complicated and costly to support.

The market is working to establish common use cases and data categories around which data providers can build their APIs to meet the needs of the market. Industry participants have been collaborating on the design and building of APIs for years through FDX, an industry standard-setting body that was established for the sole purpose of developing security protocols for APIs to facilitate a more secure connected banking ecosystem.[35] The industry collaborated through the OFX consortium for decades prior to the establishment of the FDX.[36]

The CFPB also should consider publishing model forms that could be used for the authorization process, but that would not be required to be used. These forms could include a standardized presentation that explains categorized use cases to consumers in a manner that they will easily understand. These categorized use cases could be applied by the data provider that will have to create

[35] *See* Financial Data Exchange website at https://financialdataexchange.org/.

[36] *See* OFX Work Group - About (financialdataexchange.org)

the API, while allowing sufficient flexibility to tailor the authorization to each data provider's and third party's needs.[37] The model presentation should contemplate uses on mobile screens, as well as tablet and desktops, and paper copies, and should provide sufficient flexibility to reflect the specific authorizations for the financial products and services. The CFPB should engage in copy-testing or other consumer tests to evaluate various disclosure options to ensure the final model form is one that is most helpful and clear to consumers with respect to the intended terms of authorization instead of arbitrarily deciding a single method is preferable. Proper use of the forms should satisfy any requirements regarding authorization established by the CFPB, and data providers should be able to reasonably rely on customer authorizations that are obtained using the standardized forms and be exempt from liability for any issues with the authorization if those standard presentations are used.

Data providers should have flexibility in how they meet their obligation to enable third-party data sharing through direct integrations, indirect integrations (i.e., via one or more data "aggregator" intermediaries), or a combination thereof. Any other approach would be prohibitively complicated and costly in practice to implement across the industry. There are thousands of data providers and thousands of data recipients today, and it would be prohibitively burdensome and expensive for data recipients to build thousands of direct "pipes" into each data provider. In addition, data providers incur incremental costs for each data recipient or data aggregator with whom they integrate directly, because of, among other things, costs arising from the need for support, testing, managing complaints or other issues, third-party oversight, and legal and compliance frameworks.

Data providers should further be permitted to enable data sharing with third parties through indirect integrations, for example through a central utility, such as Akoya.[38] Through Akoya, "financial institutions, fintechs, and data aggregators can enable multiple API connections" and "avoid continued maintenance and development efforts."[39] In addition, Akoya "offers a passthrough model that does not copy, store, or hold any financial data or personal information."[40] Simply stated, we advocate for a rule in which data providers are provided with flexibility in how they implement API solutions to capture and honor the customer's scope of authorization.

**b. Data providers should be able to reject a third party's request for a customer's data if certain conditions are not met.**

In addition to having the option to maintain control over the authorization process with their customers directly, data providers should have the ability to reject a third party's request to collect a customer's data for certain reasons, such as if the data provider is unable to authenticate that the requesting entity is acting on behalf of the customer or is the actual authorized third party. If data

[37] This approach would be similar to that taken by the CFPB in Regulation B, under which model Sample Notification Forms are provided in Annex C, and Annex C states that "a creditor may design its own notification forms or use all or a portion of the forms contained in this Appendix" and that "proper use" of the forms will satisfy the relevant requirements of the relevant regulations.

[38] *See* https://akoya.com/about.

[39] *Id*.

[40] *Id*.

providers require authentication, they should be able to rely on the processes they have developed and determined to be a reliable means to authenticate a third party and be free from liability for any issues that may arise from this process.

Data providers should have the right to require third parties to demonstrate that they have disclosed to the consumer, and the consumer has consented to, the third party's specific terms and conditions, which, as noted previously, should include terms of access, storage, use, including any secondary use, and disposal.[41] The terms of data access, in turn, should include access frequency, data scope, and retention period.

To protect the security and privacy of consumer data as well as their own systems, data providers should be permitted, at their discretion, to block data sharing with specific third parties where there is reasonable evidence of misuse, non-compliance with applicable laws or regulations, insufficient data privacy and security protections, or other activities that place the consumer's data, the safety and soundness of the data provider, or network integrity at risk until the issue is satisfactorily resolved. In addition, data providers should not be required to make data available to any third party that is unwilling to accept liability for loss or harm that results after the data leaves the data provider's portal (although, as discussed further below, the CFPB should establish a framework to apportion liability for loss or harm arising from data sharing between data providers and data recipients). Banks must operate in a safe and sound manner, and the CFPB should recognize that third party risk management obligations require banking organization data providers to manage who can access consumer account information and implement reasonable obligations on those entities necessary to protect the institutions' safety and soundness and customers (i.e., data security, data use, liability, audit/oversight, etc.).

**c. Consumers must have transparency into and control over the terms under which their data would be shared**.

Despite various efforts to clarify how data is used once a consumer authorizes access,[42] many consumers lack an understanding of how their financial information is being collected, shared, and stored. A December 2021 survey conducted by The Clearing House, a banking association and payments company, found that more than three-quarters of respondents were largely unaware that fintech apps:

- Commonly use third-party providers to gather users' financial data (80%)
- Can sell personal data to other parties for marketing, research, and other purposes (76%)
- Retain access to information even after the app is deleted (77%)
- Regularly access personal data even when the app is closed or deleted (78%)

[41] *See* CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Principle 3.

[42] *See*, *e.g.*, Bureau of Consumer Fin. Prot., Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation at 1; *see also*, Max Bentovim, "What to consider when sharing your financial data" (Jul. 24, 2020), available at https://www.consumerfinance.gov/about-us/blog/what-to-consider-when-sharing-your-financial-data/.

- Typically assume no responsibility if a security breach compromises consumer data (80%).[43]

To address the lack of understanding, as part of the consumer consent process, as the CFPB set forth in its Principles for Consumer-Authorized Financial Data Sharing and Aggregation, third parties should be required to provide clear disclosures regarding the "identity and security of [the] party, the data they access, their use of such data, and the frequency at which they access the data . . . throughout the period that the data are accessed, used, or stored."[44]

The CFPB asserts in the Outline that it is considering prohibiting 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 limitation standard)."[45]

We agree that the scope of data that may be collected, used, and retained by a third party will vary according to the particular use case at issue. We are concerned that permitting third parties to access information that is "reasonably necessary" to provide the service sought by the consumer is too broad and could allow third parties to collect data beyond what is necessary to provide such product or service, as "reasonableness" is open to various interpretations, and the Outline does not clearly articulate this standard. It may be useful for the CFPB to define what constitutes "reasonably necessary" with respect to common use cases and not allow inconsistent application of the standard among similarly situated entities if this standard is implemented by the CFPB.

The CFPB also should consider articulating a narrower limiting principle consistent with the principle of data minimization, which provides that the amount of data collected, used and disclosed should be limited to only that which is necessary (i.e., the minimum necessary) to provide the service the customer seeks via his or her authorization.[46] Limiting the dissemination of sensitive data reduces the consumer's risk of exposure to the data being stolen or otherwise misappropriated. The natural incentives of data aggregators and data recipients may not necessarily be aligned with this principle. The CFPB should obligate third parties to comply with data minimization requirements that apply to the collection, use and disclosure of consumer data. The CFPB's Second Principle under its Consumer Data Protection Principles is consistent with this narrow limitation, providing that "[t]hird parties with authorized access [should] ***only access the data necessary*** to provide the product(s) or service(s) selected by the consumer and [should] only maintain such data as long as necessary."[47] "Necessary" data as opposed to "reasonably necessary" would permit third parties to only collect information that is essential to provide the product or service. If this standard is adopted, the CFPB should consider articulating what is meant by "necessary" with respect to common use cases and to supervise third

---

[43] 2021 Consumer Survey: Data Privacy and Financial App Usage, December 2021, available at: 2021-TCH-ConsumerSurveyReport_Final.pdf (azureedge.net).

[44] CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Principle 6.

[45] Outline at 40.

[46] Principle 3 of Art. 5 of the GDPR, "Principles relating to processing of personal data," provides that "Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."

[47] CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Principle 2.

parties to ensure compliance with that standard.

Regardless of the use case or outer limiting bounds, the principle of consumer control over the collection and use of his or her data should govern all transactions that occur in this ecosystem. Consumers should be aware of and consent to the data that will be provided, to whom it will be provided (including downstream recipients), for how long, and for what specific purpose. Consumers can only maintain control over the sharing and use of their data if they are provided with clear, segregated disclosures from the third party (or third parties, if multiple third parties are involved in a transaction, such as a fintech company and a data aggregator) that articulate the specific data that will be collected, for what purpose, how it will be used and stored, and that clearly lay out the way(s) in which the consumer can revoke his authorization. Furthermore, data providers should have the flexibility to require third parties to demonstrate to the data provider that the customer authorized his or her information to be shared and that the third party made detailed disclosures to the customer about the collection, use, and retention of the data.

Clear disclosures by third parties regarding the use of the customer's data are of paramount importance, as many consumers are not aware who has access to their data or how their data is used, as noted previously. For example, many are unaware that deleting an app from their phone does not revoke the app's (or the app's data aggregator's, if any) ability to continue to access the consumer's financial data. Indeed, Federal Reserve Board Governor Lael Brainard has observed, "[w]hen a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information."[48]

In addition, consumers should have the ability to revoke data authorization. As the CFPB recognized in its Principles for Consumer-Authorized Data Sharing, "data revocation terms must be disclosed to the consumer, and the consumer should be able to "readily and simply revoke authorizations to access, use, or store data."[49] Consumer revocation of authorization should not necessarily lie solely with the third party, as contemplated by the CFPB in its Outline. Consumers may not remember the entities with which they have shared their data, their login credentials to all those entities, or even know who the intermediary aggregator(s) are or were. Data providers should be allowed to enable customers to manage all those permissions via the data provider's online portal. If revocation is made to the third party, data providers should have the right to require third parties to report consumer revocations within a reasonable time period (i.e., five business days). This would also support better third-party risk management and oversight, enabling further analyses, such as spike and trend reports, of revocation requests.

The right to data deletion also is an important and effective way consumers can protect themselves from future data breaches. And while the CFPB's second principle states that "[t]hird parties with authorized access … [should] only maintain such data as long as necessary," many data aggregators and data recipients may not provide consumers with the ability to easily exercise the right to deletion,

---

[48] Lael Brainard, "Where Do Consumers Fit in the Fintech Stack?" (Nov. 16, 2017), *available at* https://www.federalreserve.gov/newsevents/speech/brainard20171116a.htm.

[49] *Id*.

to the extent they provide this right at all. Governor Brainard also acknowledged this problem, noting that "[i]f a consumer severs the data access, for instance by changing banks or bank account passwords, it is also not clear how he or she can instruct the data aggregator to delete the information that has already been collected. Given that data aggregators often don't have consumer interfaces, consumers may be left to find an email address for the data aggregator, send in a deletion request, and hope for the best."[50] Thus, the CFPB should require nonbank third parties to provide consumers with a simple, clear way to request that their data be deleted by the nonbank third party.

**c. Data providers should be permitted to impose reasonable time, place, and manner restrictions on data access.**

The CFPB's Outline provides that "[t]he CFPB is considering proposing that authorized third parties would be limited to accessing consumer-authorized information for only as long (duration) and as often (frequency) as would be reasonably necessary to provide the product or service the consumer has requested. The CFPB is also considering proposing that the authorized duration would be limited to a maximum period, after which third parties would need to seek reauthorization for continued access. These proposals would seek to ensure the third party is not accessing information beyond what the consumer intended to authorize and ensure that third parties do not continue to access information for a product or service that the consumer no longer uses. Limiting duration and frequency in this way could ensure access for a variety of consumer-requested use cases and protect consumers from risks related to open-ended access."[51]

BPI supports the ability of data providers to collect consumer reauthorization on a periodic basis, as well as limitations on duration and frequency of access. The CFPB should subject third parties to regulation and examination to ensure that those entities only seek access for as long and as often as would be ***necessary***, as opposed to "reasonably necessary," as the latter standard could allow for duration and frequency of access beyond what is necessary to provide the customer with the product or services he seeks, which could harm consumers. Should a third party seek to collect information beyond what is "necessary" to provide the desired service, the CFPB should have the authority to impose penalties on such third party under the supervisory and examination authority it should establish over such entities, as described further below.

Even with such limitations, there is a risk that the cumulative volume of third-party traffic could overwhelm and negatively impact the functioning of data providers' systems. As such, data providers should be permitted to implement reasonable time, place, and manner restrictions, including reasonable restrictions on access to their own API to protect customers and infrastructure when needed. Data providers should not be required to meet higher standards for availability or other terms for a third-party data channel (where a customer is not always "present" in the flow) than for first-party digital channels for customers (where the customer is always present in the flow). However, if the CFPB were to implement a requirement that data providers adhere to service level agreements, data providers may have to incur significant costs, including for measuring and demonstrating compliance with SLA requirements. If this requirement were implemented, data providers should be permitted to

[50] *Id*.

[51] Outline at 41.

charge reasonable fees to third parties to recover costs associated with adhering to service level agreements. Fees for access requests are common among similar frameworks that grant access rights to individuals and/or third parties and generally permit entities to charge a reasonable fee based on administrative costs and in some cases, the ability to charge additional fees or even deny access in the event of excessive requests.

## V. Data aggregators should be subject to CFPB supervision and examination.

The CFPB states that "nearly all—if not all," third party market participants are subject to GLBA.[52] Yet the FTC, not the CFPB, has interpretive authority over the application of GLBA to nonbank entities. Therefore, to effectuate the application of GLBA to third parties and create a level playing field for the parties that will be accessing consumer personal financial data, which we support, the CFPB should coordinate with the FTC to require all third-party data recipients to comply with the requirements of GLBA, which should be laid out explicitly in the CFPB's rulemaking under section 1033 or otherwise made clear. However, data providers should still have discretion to implement bilateral data sharing agreements that contain additional data security, privacy or other requirements.

In addition, merely subjecting third parties to those requirements is not sufficient to ensure that they are followed. The CFPB has the authority under the Dodd-Frank Act to define the universe of larger nonbank participants in the market for data aggregation services. The CFPB should initiate a rulemaking under this authority to designate third party data aggregators and data users, or determine, by order, that such entities are engaging, or have engaged, in conduct that poses risks to consumers, which would then give the Bureau the authority to supervise and examine those entities for compliance with applicable data security standards and federal consumer protection laws, just as banks are regularly examined for compliance with these laws.[53] The FFIEC exam guidance on information security also could serve as a useful model for the Bureau in developing the appropriate information security standards for large nonbank data aggregators and data users.[54]

Only by subjecting these entities to the same data privacy and security requirements and expectations to which banks are subject, as well as supervision and examination for complying with

---

[52] Outline at 45.

[53] 12 U.S.C. 5514(a)(1)(B), (a)(2), (a)(1)(C). *See "*Petition to The Consumer Financial Protection Bureau for rulemaking defining larger participants of the aggregation services market," American Bankers Association, Consumer Bankers Association, Credit Union National Association, Housing Policy Council, Independent Community Bankers of America, National Association of Federally-Insured Credit Unions, National Bankers Association, and The Clearing House Association (August 2, 2022), available at: Regulations.gov; *see also* BPI comment letter in support of the joint trades petition for rulemaking defining larger participants of the aggregation services market (Oct. 3, 2022), available at: BPI-CFPBcommentreDataAggregatorPetitionforRulemaking-2022.10.03.pdf.

[54] FFIEC, Information Technology Examination Handbook, Information Security Booklet, *available at* https://ithandbook.ffiec.gov/it-booklets/information-security.aspx

those requirements and expectations, can consumer data be sufficiently protected within the consumer financial services marketplace.[55]

Data providers also should have the flexibility to require third parties to meet additional data security and privacy requirements as a condition of providing them with customer information. This flexibility is particularly important so long as there is no liability framework in place to fairly apportion liability for consumer loss or harm among data providers and third parties.

## VI. The CFPB should fairly apportion liability among data providers and data recipients.

Although the topic of liability within the data sharing ecosystem is of critical importance and has been subject to significant discussion among the relevant stakeholders, the CFPB's Outline is silent on this topic. It is essential that the CFPB address the question of liability for loss or harm caused by the entity with possession, custody or control over the data or which is otherwise responsible for the loss or harm. For data providers, any liability for any incident leading to loss or harm should end when the data leaves the data provider's portal. Without a universal framework for apportioning liability, parties must apportion liabilities and indemnities in bilateral contracts. If the CFPB decides to address liability, the rule should place liability for any loss or other harm on the entity with possession, custody or control over the data or that is otherwise responsible for the loss or harm.

Because banks' relationships with their customers are built on trust, and because banks seek to provide their customers with outstanding customer service, customers will likely look to their bank rather than the data recipients to make them whole for a loss or other harm that befalls the customer despite the fact that the customer harm occurred after the customer's data left the data provider's by portal, and the bank could not prevent the harm. For this reason, data providers should be indemnified by the party responsible for any costs the data provider incurs resulting from any loss or harm that arises after the customer's data has left the data provider's portal.

The third parties in this data sharing ecosystem have represented that they are agents, representatives, or, otherwise acting on behalf of the consumer and thus are able to access the consumer's data on their behalf pursuant to 1033. Under agency theory, third party data users or data aggregators that access a consumer's data as the agent for the consumer shall indemnify the consumer acting as the principal if the agent fails to discharge its duties with the appropriate standard of care and such failure results in a breach or unauthorized use or disclosure of the consumer's data. This may include third parties in the process with whom neither the data provider nor the consumer has a direct relationship (such as a data aggregator that uses another data aggregator's APIs to obtain access to

[55] The CFPB's has entered into limited privacy and security enforcement actions, most notably in its Consent Order with Dwolla, Inc., in which the CFPB used its authority to prohibit unfair, deceptive, or abusive acts or practices to impose prescriptive data security requirements on Dwolla, including with respect to customer identity authentication. *See* Consent Order, *In re Dwolla, Inc*., File No. 2016-CFPB-0007 (Mar. 2, 2016). Subjecting third parties to comprehensive CFPB supervision and examination for their data security practices would benefit consumers by helping to ensure that those practices are compliant with the relevant requirements before consumer harm has occurred as compared to individual actions reacting to alleged unfair deceptive, or abusive acts or practices after consumer harm may already have occurred.

consumer personal financial data). The CFPB should make this standard of care clear so that all parties within the ecosystem understand the obligations, responsibilities, and liabilities if a third party allegedly fails to act with the appropriate standard of care when acting as the consumer's agent in the data sharing ecosystem. Indemnification, as a method to apportion liability, will have the added benefit of incenting relevant third parties to enhance their data security and privacy practices to help prevent customer harm for which they could be held liable.

## VII. Data providers should have flexibility to determine what information to share with third parties.

Section 1033(a) requires covered persons to "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 . . . ." The CFPB is considering expanding the scope of data that a covered data provider would be required to make available to a consumer or third party beyond what is contemplated by the statute and beyond what is necessary to provide the consumer with a desired product or service. Information that is made available to third parties should be consistent with the principle of data minimization: third parties should be able to collect only that information that is necessary to provide the consumer with the desired product or service.

The Outline sets forth six categories of information the CFPB is considering requiring covered data providers to make available with respect to covered accounts:

1. Periodic statement information regarding transactions and deposits that have settled, including fees, account terms and conditions, and the annual percentage yield of an asset account or the annual percentage rate of a credit card account;

2. Information regarding prior transactions and deposits that have not yet settled;

3. Information about prior transactions not typically shown on periodic statements or online financial account management portals;

4. Online banking transactions that the consumer has set up but that have not yet occurred;

5. Account identity information; and

6. Other information, including consumer reports obtained and used by the covered data provider in deciding whether to provide an account or other financial product or service to a consumer; fees that the covered data provider assesses on its consumer accounts; bonuses, rewards, discounts, or other incentives that the covered data provider gives to consumers; and information about security breaches that exposed a consumer's identity or financial information.

Some information the CFPB is contemplating requiring data providers to share would go well beyond information in the control or possession of the covered person and would be inconsistent with the important principle of data minimization and would not appear to advance the purpose of section 1033, as articulated by the CFPB, to promote competition in the consumer financial services markets. In

addition, covered data providers may not have the information in the enumerated items (1)-(6) above readily available in their control or possession. Requiring covered data providers to obtain such information would hinder the CFPB's objectives of providing consumers with quick and efficient access to their consumer personal financial data.

In general, data providers, working with their customers, should have flexibility to determine what information to provide to a third party that would be necessary to provide the consumer the product or service he is seeking.

BPI members generally currently make available to third parties information that appears on periodic statements that they are required to provide for asset and credit card accounts (as only those are currently contemplated to be covered as "data providers") to facilitate consumers' access to products and services offered by third parties. Therefore, data providers would likely not face issues making information on the periodic statement available to third parties, so long as that information is necessary to provide the product or service sought by the customer (subject, of course, to customer authorization). For other data providers that the rule should be expanded to cover, information that is provided periodically to consumers in the control or possession of the data provider concerning the consumer financial product or service would be appropriate to provide to third parties if it is necessary to provide the desired product or service.

Data providers should have the flexibility, but not be required, to provide additional information to third parties, as discussed in more detail below. The CFPB should consider working with industry and other stakeholders to standardize data across market participants and aligned with existing regulations in order to reduce implementation frictions and costs.

We address each of the proposed categories in more detail below.

**a. Periodic Statement Information for Settled Transactions and Deposits.**

The Bureau is considering requiring covered data providers to make available the 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[56] and for credit card accounts.[57] The Outline states that data elements in this category would include the following:

- 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;
- Any fees charged to the account;
- Any interest credited to an asset account or charged to a credit card account;
- The annual percentage yield (APY) of an asset account or the annual percentage rate (APR) of a credit card account;

[56] The Outline notes that this information is required under Regulation E § 1005.9(b) and under Regulation DD § 1030.6(a). Regulation DD applies to depository institutions except for credit unions. See § 1030.1(c).

[57] Outline at 19. The Outline notes that this information is required under Regulation Z §§1026.7(b) and 1026.8.

- The current account balance;
- 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);
- The terms and conditions of the account, including a schedule of fees that may be charged to the account;
- 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
- For an asset account, the account number as required by Regulation E.[58]

This information is consistent with the statutory requirement that data providers provide "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." To the extent that this information, or some subset of this information, is necessary to provide the consumer with the product or service he seeks, it would seem appropriate to make this information available to a consumer or to an authorized third party. BPI members generally make this information available to consumers and to authorized third parties currently. Data providers should have the option to share a tokenized deposit account and routing number in lieu of the "real" deposit account number to authorized third parties. The industry is moving toward tokenization of deposit account and routing numbers to provide greater customer protection and control and reduce fraud. A requirement that banks share real deposit account numbers would introduce significant and unnecessary risk into the payments ecosystem. Fraud is at an all-time high and the industry is evolving away from the use of deposit account numbers and other access credential information for certain functions to help reduce fraud.[59]

**b. Information regarding prior transactions and deposits that have not yet settled.**

The CFPB is considering requiring covered data providers to make available information regarding transactions and deposits that have not yet settled. The Outline states that "the data elements about approved but not settled transactions and deposits that the CFPB is considering proposing be made available are typically shown to consumers in the transaction history that covered data providers make available through their online financial account management portals."[60]

Sharing pending transaction details may unnecessarily introduce unreliable data into the ecosystem. For example, pending transactions and deposits often change considerably after settlement and thus sharing this data prematurely could cause customer confusion. While this information may concern the consumer financial product or service that the consumer obtained from the data provider, it is not clear how this information would be necessary for any particular product or service that a

[58] Outline at 19-20.

[59] *See* Federal Trade Commission, "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021: Reported fraud losses increase more than 70 percent over 2020 to more than $5.8 billion" (Feb. 22, 2022), available at: New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021 | Federal Trade Commission.

[60] Outline at 20.

consumer may seek from a third party. Nor does the CFPB articulate how the provision of this data to third parties would further the goal of enhancing competition in the consumer financial services marketplace.

For the foregoing reasons, mandating the sharing of this type of information would be problematic and would likely pose risks to consumers that do not appear to be outweighed by any potential benefits. Data providers should not be required by regulation to provide this information to third parties, but instead, the market should be permitted to determine if this type of data is necessary and useful to provide consumers with access to desired products and services.

**c. Other information about prior transactions not typically shown on periodic statements or portals**.

The "CFPB is considering proposing that covered data providers would need to make available information about prior transactions that covered data providers typically do not display on periodic statements or online financial account management portals," which may include certain data "from the payment networks in which they participate" about transactions "that are not reflected on the periodic statement or portal."[61] The CFPB states that card networks, ATM networks, automated clearing house (ACH) networks, check-collection networks, and real-time payment networks are "examples of the payment networks in which a covered data provider would typically participate, and which provide transaction-specific data to the covered data provider."[62]

The CFPB states 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."[63]

The CFPB explains further that many "of the data elements covered data providers receive from payment networks . . . may be helpful to consumers as they seek to exercise their rights with respect to payments, including fraudulent or otherwise erroneous payments, that may be charged to their accounts."[64] For the reasons provided below, the CFPB should not require data providers to share data on prior transactions that data providers typically do not display on periodic statements or online portals.

The statute requires consumers to be provided "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." The information contemplated in this category, however, may not be in the

[61] *Id*.

[62] *Id*.

[63] Outline at 21.

[64] *Id*.

control of the data provider. Furthermore, the disclosure of this information, particularly names and account numbers of the payment recipient, would be highly problematic, as this data can be used to facilitate fraud.

The CFPB asserts that this information may be helpful to consumers "as they seek to exercise their rights with respect to payments, including fraudulent or otherwise erroneous payments," but does not explain why the current laws, regulations, and mechanisms for addressing fraud or erroneous payments are insufficient, or how this additional information would assist consumers beyond what these mechanisms available to them today. Banks provide extensive customer support services to assist customers with all manner of issues, including transaction disputes that may involve allegations of fraud. Furthermore, under Regulation E, consumers are not liable for unauthorized transactions. Many banks provide reimbursement beyond what is required by law and regulation. Requiring data providers to make this information available would impose a substantial burden on data providers for an unclear benefit.

For the foregoing reasons, mandating the sharing of this type of information would be problematic and could pose risks to consumers that do not appear to be outweighed by any potential benefits. Data providers should not be required by regulation to provide this information to third parties, but instead, the market should be permitted to determine if this type of data is necessary and useful to provide consumers with access to desired products and services.

**d. Online banking transactions that the consumer has set up but that have not yet occurred**

The CFPB also is considering proposing that covered data providers would need to make available information regarding banking transactions a consumer has set up but that have not yet occurred. Data providers should not be required to disclose such information. First, potential privacy concerns would arise should the CFPB require this information to be disclosed, such as bill pay data that includes sensitive personal information of a customer's payees (including, but not limited to, home address and bank account numbers). Second, the existing market demand for this information is not sufficient to justify the costs associated with making these data elements available to consumers. Data providers would be required to incur substantial costs to operationalize these new data elements, and to date, BPI members have seen insufficient market demand to justify these costs. Third, there is no mechanism to rationalize recurring billers at one institution being shared and set up at another provider, which could lead to issues of double payment and potential overdrafts.

For the foregoing reasons, mandating the sharing of this type of information would be problematic and would likely pose risks to consumers that do not appear to be outweighed by any potential benefits. Data providers should not be required by regulation to provide this information to third parties, but instead, the market should be permitted to determine if this type of data is necessary and useful to provide consumers with access to desired products and services.

**e. Account identity information**

The CFPB is considering requiring covered data providers to make available information related to the identity and characteristics of the consumer accountholder. The CFPB lists the following information that may be required to be provided under this category:

- Name
- Age
- Gender
- Marital status
- Number of dependents
- Race
- Ethnicity
- Citizenship or immigration status
- Veteran status
- Residential address
- Residential phone number
- Mobile phone number
- Email address
- Date of birth
- Social Security number
- Driver's license number.

The CFPB asserts that this type of information "could be useful to an authorized third party seeking to verify a consumer's ownership of an account with a covered data provider, whether for purposes of an interaction with the covered data provider or with another entity, such as a potential lender."[65] While the CFPB acknowledges that sharing this type of information raises "fraud, privacy, and other consumer protection risks," the CFPB states that "these risks could be at least somewhat mitigated through a "confirm/deny" approach under which an authorized third party, seeking to verify consumer account ownership, would present to a covered data provider the identity information that the consumer provided to the authorized third party . . . [and] the covered data provider . . . could merely confirm or deny that the information presented by the authorized third party matches the information that the covered data provider has on file about the consumer."[66]

For several reasons, data providers should not be required to share the majority of this information. We agree that basic identity information – name, address, phone number, email address – may be useful in verifying account ownership, but the rest of this information is highly sensitive demographic information that should not be subject to data sharing. In addition, much of this information is not readily collected in a format that is easily transmittable to a third party. This data does not appear to provide any measurable value to a consumer in terms of receiving a financial product or service, and sharing this type of data could raise challenges with respect to maintaining accuracy as the data is transmitted from one party to another.

[65] Outline at 23.

[66] *Id*.

The statute states that data providers shall provide consumers "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." Account identity information does not concern the "consumer financial product or service" but rather relates only to the consumer herself. Furthermore, this data is readily available directly from consumers if they choose to share it. Requiring consumers to share this information directly notifies them that a third party intends to use their sensitive personal demographic information in connection with a financial product or service the consumer is enrolling in and enables the customer to have control over sharing that information, consistent with the fundamental principle of ensuring that consumers have ultimate control over their data. Furthermore, some of the data within this category is susceptible to becoming stale, raising concerns about poor data quality and accuracy.

Sharing account identity information is likely to increase the risk of bad actors using that data to engage in synthetic identity theft. The increase in the risks to the security of consumer data and the implementation complexity that would be required to share this expanded scope of data may not be warranted in relation to the benefit, which in many cases is not clear. For example, the benefits of sharing sensitive personal information like demographic information and Social Security numbers are not obvious, while the risks of sharing this information are real and numerous. Furthermore, some of this sensitive information, such as race, is not collected by data providers generally.

As noted, the CFPB states that the risks of sharing sensitive customer information "could be at least somewhat mitigated through a "confirm/deny" approach. However, requiring data providers to support platforms or APIs that confirm or deny user-submitted identity information would require highly complex updates to current platforms and would not produce enough consumer benefit to warrant the cost. Tools that would confirm or deny a "match" between user-submitted identity data across systems are hard to operationalize in practice, and many market participants lack confidence in this "matching logic" provided by an outside entity (in this case, the data provider, necessarily) and thus do not use this process in their own business applications for risk management and identity verification purposes.

For the foregoing reasons, mandating the sharing of this type of information would be problematic and would likely pose risks to consumers that do not appear to be outweighed by any potential benefits. Data providers should not be required by regulation to provide this information to third parties, but instead, the market should be permitted to determine if this type of data is necessary and useful to provide consumers with access to desired products and services.

**vi**. **Other information**

The CFPB is considering proposing that covered data providers would have to provide other information they might have about their consumer accountholders. Specifically, the CFPB is considering proposing that covered data providers would need to make available:

- Consumer reports from consumer reporting agencies, such as credit bureaus, obtained and used by the covered data provider in deciding whether to provide an account or other financial product or service to a consumer;
- Fees that the covered data provider assesses in connection with its covered accounts;

- Bonuses, rewards, discounts, or other incentives that the covered data provider issues to consumers; and
- Information about security breaches that exposed a consumer's identity or financial information.

The CFPB provides no explanation for why it is proposing that data providers be required to make this information available. Many fees charged on covered accounts are subject to disclosure requirements under other laws and regulations.[67] In addition, consumers have separate statutory rights to obtain their consumer reports directly from the CRAs, and lenders are subject to a comprehensive regulatory regime under the FCRA and Regulation B to notify consumers when their credit report is being pulled, when an adverse action is taken, and about the ability to obtain free credit reports.[68]

Furthermore, data providers that are banks are required to provide information about security breaches to their customers and regulators under various laws and regulations.[69] For example, in 2021, the federal banking agencies finalized incident notification requirements to a banking organization's primary federal regulator that are triggered upon a determination that a computer-security incident has occurred that has caused, or is reasonably likely to cause actual harm to the institution's operations and ability to deliver products and services to a significant portion of its customers, or could pose a risk to the financial stability of the United States.[70] Pursuant to GLBA, banks are required to notify their customers when an incident has occurred involving the unauthorized access or use of the customer's information, the requirements of which are set forth in the federal banking agencies' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.[71] Rather than require data providers to provide incident reports to third parties, third parties should be held to the same notification requirements to relevant regulators and consumers as banks, and the CFPB should supervise and examine those entities for compliance with those requirements.

---

[67] Comprehensive consumer fee disclosure statutes and regulations administered by the CFPB include: (i) the Truth in Lending Act and Regulation Z, 15 U.S.C. § 1601 *et seq.* and 12 CFR 1026; (ii) the Real Estate Settlement Procedures Act and Regulation X, 12 U.S.C. § 2601 *et seq.* and 12 CFR 1024; (iii) the Electronic Fund Transfer Act and Regulation E, 15 U.S.C. § 1693 *et seq.* and 12 CFR 1005; (iv) the Truth in Savings Act, 12 U.S.C. § 4301 *et seq.* and 12 CFR 1030; and (v) Consumer Leasing Act and Regulation M, 15 U.S.C. § 1667 *et seq.* and 12 CFR 1013. TILA requires fee disclosures for all types of consumer credit products including credit cards, mortgages, auto loans, and installment loans, while TILA and RESPA collectively require mortgage and mortgage closing disclosures. The EFTA and TISA collectively require fee disclosures related to deposit products, electronic fund transfers, overdrafts, remittance transfers, prepaid cards, and gift cards. The CLA requires fee disclosures related to consumer leases.

[68] *See* 15 U.S.C. § 1681 et. seq. and 12 CFR 1022 *et. seq*.

[69] See, e.g., OCC Bulletin 2021-55, available at: https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-55.html; Cal Civ. Code § 1798.80 et seq., Del. Code Ann. Tit. 6 §12B-101 et seq., 815 Ill. Comp. Stat. 530/5 et seq., N.Y. Gen. Bus. Law § 899-aa.

[70] *See* 86 Fed. Reg. 66424 (Nov. 23, 2021), available at: 2021-25510.pdf (govinfo.gov).

[71] *See* Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); Office of Thrift Supervision, Treasury (OTS), "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," 70 Fed. Reg. 15736 (March 29, 2005), available at: 05-5980.pdf (govinfo.gov).

For the foregoing reasons, mandating sharing of this type of information would be problematic and would not appear to be outweighed by any potential benefits. Data providers should not be required by regulation to provide this information to third parties, but instead, the market should be permitted to determine if this type of data is necessary and useful to provide consumers with access to desired products and services.

## VIII. The CFPB should prohibit reverse engineering of confidential commercial information.

The CFPB's rules should clearly prohibit access to confidential commercial information and clarify that using disclosed data elements to reverse engineer underwriting algorithms or other confidential commercial information is prohibited. Section 1033(b) protects against sharing confidential commercial information, but a large-scale sharing of data that contains the output of confidential or proprietary models creates a serious risk to the protection of the models themselves through reverse engineering. The CFPB's Outline is concerning in that it proposes expansive data sharing for bank and credit card accounts while merely restating the statutory protection in Section 1033(b). The CFPB offers no analysis and no policy suggestions to prevent obtaining confidential commercial information through reverse engineering.

The Dodd-Frank Act makes clear that data providers may not be required to make available to the consumer "any confidential commercial information, including an algorithm used to drive credit scores or other risk scores or predictors."[72] Though the statute was written before "Big Data," any regulations by the CFPB must recognize that providing disclosures directly to individual consumers is fundamentally different from providing data indirectly to consumers via third parties, particularly at scale, even if those third parties collect data as agents for individual consumers.

Large-scale sharing of data that contains the output of confidential models, such as credit or risk scores, raises significant concerns about the protection of the underlying confidential models themselves. Statisticians using traditional regression analysis have long used a "one in ten" rule of thumb for the proposition that it only requires ten events (e.g., ten consumers' data) to accurately determine the weight for each predictive variable studied. The ease with which confidential information can be reverse engineered from algorithmic outputs has since been extended to a wide range of machine learning types, such as decision trees and even deep neural networks.[73] Individual data aggregators have pulled data from as many as 40 percent of American bank accounts. If highly complex machine learning algorithms can be reverse-engineered with relatively limited data, third parties such as data aggregators and data users would likely be able to reverse-engineer data providers' credit or risk scoring algorithms, precisely the type of information protected from sharing under section 1033.

Even if the output of a confidential algorithm is not produced as a specific data field, in many

[72] 12 U.S.C. § 5533(b).

[73] In 2016, researchers were able to recreate confidential commercial algorithms by major machine-learning-as-a-service operators, including Amazon, with less than 4,500 queries -- and in some cases, as few as 650. Florian Tramer, Fan Zhang, Michael Reiter, Thomas Ristenpart, Stealing Machine Learning Models via Prediction APIs, Proceedings of the 25th USENIX Security Symposium (Aug. 2016) https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_tramer.pdf.

cases, the confidential algorithm's output can be proxied or otherwise reverse-engineered using other transaction data. For example, APR can be determined by interest charges and balances observed. An automobile loan provider's approach to lending against collateral could be reverse-engineered using the Vehicle Identification Number often included in auto loan statements. Even if a data recipient does not copy a confidential algorithm (i.e., a set of calculations returning a range of outputs based on particular inputs), a data recipient can copy a confidential algorithm's outputs. For instance, a data recipient could build a crude, but effective, credit model by monitoring a consumer's credit transactions for events that reflect algorithmic decisions from the data provider, such as changes to APR or credit lines. The data recipient would not have technically copied the data provider's credit model as it would not use the same inputs that the data provider used in building the model (e.g., credit scores, transaction data, risk metrics). Rather, the data recipient would use transaction data, which would necessarily reflect the data provider's determination of credit risk for that consumer.

If the CFPB is going to consider facilitating disclosure to consumers and third parties authorized by consumers to act on their behalf of the outputs of confidential commercial algorithms (e.g., interest rates, credit limits, and certain fees), any such disclosure must be paired with categorical prohibitions on how such data may be used by third parties such as data aggregators and data users. Because algorithm outputs can be proxied or reverse-engineered by other transaction data, these use-case prohibitions must apply to transaction data as a whole. Such use restrictions would not interfere with individual consumers' ability to receive relevant information about their financial products and services as contemplated by section 1033, while ensuring the integrity of confidential commercial information.

Prohibitions on reverse-engineering are standard components of developer agreements, and large data aggregators themselves uniformly require such commitments in their agreements with data recipients.

## IX. Banks should not be required to share customer information in a manner that conflicts with their obligations to operate in a safe and sound manner and protect consumer data.

Under the law, insured depository institutions are required to operate in a safe and sound manner.[74] The federal banking agencies have stated that "[w]hether a banking organization conducts activities directly or through a third party, the banking organization must conduct the activities in a safe and sound manner and consistent with applicable laws and regulations, including those designed to protect consumers.[75] The OCC has noted that third party risk management guidance is specifically applicable to business relationships with data aggregators and that banks have a responsibility "to manage these relationships in a safe and sound manner with consumer protections."[76]

---

[74] *See, e.g.*, 12 U.S.C. § 1831p–1, which requires each federal banking agency to establish certain safety and soundness standards by regulation or by guidelines for all insured depository institutions.

[75] The Board of Governors of the Federal Reserve System. the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38182, 38184 (July 19, 2021), available at: 2021-15308.pdf (govinfo.gov).

[76] OCC Bulletin 20220-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (March 5, 2020), available at: Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 | OCC.

The OCC has further made clear that certain 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:

> While screen-scraping activities typically do not meet the definition of business arrangement, banks should engage in appropriate risk management for this activity. Screen-scraping can pose operational and reputation risks. Banks should take steps to manage the safety and soundness of the sharing of customer-permissioned data with third parties. Banks' information security monitoring systems, or those of their service providers, should identify large-scale screen scraping activities. When identified, banks should take appropriate steps to identify the source of these activities and conduct appropriate due diligence to gain reasonable assurance of controls for managing this process. These efforts may include research to confirm ownership and understand business practices of the firms; direct communication to learn security and governance practices; review of independent audit reports and assessments; and ongoing monitoring of data-sharing activities.[77]

The federal banking agencies proposed amendments to this Guidance in 2021 and requested comment on, among other things, the extent to which banking organizations may have "business arrangements" and third-party relationships with data aggregators, and therefore should manage these relationships consistent with the third-party risk management guidance."[78]

BPI submitted a comment in response to the proposed amendments, emphasizing, among other things, that data aggregators can pose meaningful risks to banking organizations and their customers, but that the TPRM practices and expectations are not the appropriate means to address those risks.[79]

Rather, consistent with banks' important obligations to protect their customers and their own safety and soundness, the CFPB should recognize that third party risk management obligations require banking organization data providers to manage who can access consumer account information and implement reasonable contractual obligations on those entities necessary to protect the institutions' safety and soundness and customers (i.e., data security, data use, liability, audit/oversight, etc.). Indeed, section 1033(e) of the Dodd-Frank Act requires the CFPB to coordinate with the federal banking agencies and the FTC with respect to promulgating rules under section 1033.

To protect the security and privacy of consumer data as well as their own systems, data providers should be permitted to restrict access by third parties that do not meet certain minimum requirements. For example, data providers should not be required to make data available to any third

---

[77] Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38182 (July 19, 2021), 38197-38198, available at: 2021-15308.pdf (govinfo.gov).

[78] *Id*. at 38197.

[79] The ultimate expectations of the regulators in this regard remain unclear at this point. *See* BPI's comment letter in response to the "Proposed Interagency Guidance on Third-Party Relationships," available at: Microsoft Word - BPI Comment Letter - Interagency Guidance on Third Party Relationships (Docket ID(7661407.20).docx.

party that is unwilling to accept liability for any negative outcomes that may occur after a customer's data has left the data provider's portal or that does not meet sufficient data security requirements as determined by the data provider.

The CFPB and the federal banking agencies should not impose the responsibility for supervising third parties, including fintechs and data aggregators, on bank data providers. Rather, the CFPB should supervise and examine data aggregators that are larger participants in the relevant market or that could pose consumer risk, and data aggregators should be required to ensure downstream data recipients employ sufficient data security practices.

## X. The CFPB lacks authority to impose accuracy requirements.

The Outline states that the "CFPB is considering whether covered data providers should be required to make information available to third parties when the covered data provider knows the information requested is inaccurate."[80] The statute generally requires covered data providers to make available information in their control or possession concerning the consumer financial product or service that the consumer obtained from such data provider. The statute does not reference data accuracy. By contrast, for example, the FCRA and Regulation V impose accuracy requirements on the information furnished to and provided by consumer reporting agencies.[81] Congress could have included data accuracy responsibilities for data providers but did not do so. A requirement related to data providers' making determinations regarding whether information can or should be shared based on an accuracy assessment would be an impermissible expansion of the scope of the statute.[82]

There are existing methods for customers of bank data providers to address with the bank any data inaccuracies. In addition, the Outline would not impose any data accuracy requirements on authorized third parties, but rather would require them only to maintain reasonable policies and procedures designed to ensure they collect accurate information. Thus, any accuracy requirements imposed on data providers would be another example of the CFPB's imposing disproportionate obligations on data providers compared to data recipients. The CFPB should consider imposing a requirement on third party data users to ensure that the information obtained from the data provider is accurate and fit for purpose.

---

[80] Outline at 30.

[81] The FCRA provides that "[w]henever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates." 15 U.S.C. 1681e(b). Regulation V requires information furnishers to "establish and implement reasonable written policies and procedures regarding the accuracy and integrity of the information relating to consumers that it furnishes to a consumer reporting agency." 12 CFR 1022.42.

[82] Footnote 50 in the Outline notes that state privacy laws enacted in California, Colorado, and Virginia provide consumers the right to correct inaccurate personal information, but financial institutions regulated by GLBA and nonpublic personal information collected pursuant to GLBA are generally exempt from these requirements. However, these state laws of course do not provide the CFPB the authority to impose accuracy or correction requirements on data providers under section 1033; thus, any such requirements would be outside of the CFPB's authority to impose under Section 1033.

## XI. The CFPB lacks authority to impose record retention obligations.

The Outline states that the:

> "CFPB is considering proposing record retention requirements for covered data providers and authorized third parties to demonstrate compliance with certain requirements of the rule. A record retention requirement would assist with the CFPB's ability to monitor compliance with the rule and therefore better protect consumers. A record retention requirement could also assist entities in assessing their compliance with the rule. The CFPB recognizes that imposing a record retention requirement would likely increase burden on covered data providers and authorized third parties (relative to how such entities currently operate)."[83]

Section 1033 generally requires data providers to make available information in their control or possession concerning the consumer financial product or service that the consumer obtained from such data provider and imposes no requirement to maintain records. The statute also provides that it shall not "be construed to impose any duty on a covered person to maintain or keep any information about a consumer," explicitly forbidding such a requirement. Congress could have included record retention responsibilities for data providers but did not do so. For example, under the FCRA and Regulation V, creditors are required to maintain certain types of information for specified periods of time.[84]

Imposing record retention requirements would impermissibly expand the scope of the statute. Data providers of course have flexibility to implement their own record retention practices.

## XII. The CFPB should provide a more accurate estimate of the costs data providers would incur under the proposal.

The CFPB dramatically underestimates the costs for data providers to build and maintain a third-party data sharing channel. Additionally, for data providers that are already supporting third-party data sharing channels today, their costs would be much higher were they to be required to support some of the CFPB's proposals, including: (1) expansion of the mandatory data elements; (2) changes in how authorization is collected; (3) requirements to expand frequency of access and/or channel uptime; (4) failure to allow reasonable time/place/manner restrictions by data providers; and (5) changes that would increase the number of third parties each data provider would be required to integrate with directly.

The CFPB should engage in a more accurate estimation exercise to determine the costs that data providers would likely incur and balance those against the potential benefits of the proposed requirements in issuing any proposed rule.

*****

[83] Outline at 48.

[84] 12 CFR 1002.12.

BPI appreciates the opportunity to provide comments to the CFPB and would welcome the opportunity to discuss them further with CFPB staff. If you have any questions, please contact me by phone at 703-887-5229 or by email at paige.paridon@bpi.com.

Sincerely,

/s/ Paige Pidano Paridon

Paige Pidano Paridon
Senior Vice President,
Senior Associate General Counsel
*Bank Policy Institute*