BANK POLICY INSTITUTE

February 4, 2021

Via Regulations.gov

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

Re: Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (Docket No. CFPB-2020-0034)

To Whom It May Concern:

The Bank Policy Institute[1] appreciates the opportunity to comment on the Advanced Notice of Proposed Rulemaking[2] issued by the Consumer Financial Protection Bureau seeking input on consumers access to financial records pursuant to Section 1033 of the Dodd-Frank Act.

BPI commends the CFPB for taking steps to address the financial data sharing marketplace and appreciates how the CFPB's actions to date have enabled industry to move data sharing practices forward with limited regulatory intervention. Given the potential importance of Section 1033 in furthering a consumer's right to access information about a consumer financial product or service that the consumer obtained from a bank or other covered person, including information relating to any transaction, or series of transactions, to the account including costs, charges, and usage data, BPI supports the CFPB's efforts to ensure consumers retain such access, but believes that such access should be provided in a manner that appropriately safeguards consumer data.

The CFPB has an opportunity to enhance the protections applicable to consumer authorized financial data sharing, allowing for further transparency regarding their data for consumers. To this end,

---

[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 small business loans, and are an engine for financial innovation and economic growth.

[2] Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (November 6, 2020) (hereafter "ANPR").

the CFPB should consider the following overarching principles in promulgating any potential rulemaking:

- Coordination with Other Regulators. As an initial principle, it is important for the CFPB to coordinate its efforts to implement Section 1033 with the other prudential regulators, as well as the Federal Trade Commission, given that the CFPB's primary authorities do not extend over all operational risks related to such data sharing. Section 1033(e) specifically requires that the CFPB consult with Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and the FTC to ensure consistency in any promulgated rule across various types of covered persons. Additionally, the CFPB has limited jurisdiction under the Gramm-Leach-Bliley-Act ("GLBA"), which directly relates to the sharing and safeguarding of consumer financial data. The CFPB shares GLBA rulemaking authority with the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the FTC. As such, BPI recommends that the CFPB coordinate with the prudential banking agencies, FTC, SEC, and CFTC to ensure coordinated efforts in any potential rulemaking.

- Sufficient Flexibility and Innovation in the Marketplace. The CFPB's efforts to set standards for consumer authorized data sharing should ensure sufficient flexibility and innovation in the marketplace. The financial services industry continues to collaborate to develop technical solutions that enable consumer access to financial data while ensuring appropriate consumer protections. These efforts include the development of common technical standards for the secure access of consumer-permissioned data. BPI believes that industry-led standards setting bodies are best positioned to unify the financial industry around common and interoperable technical standards while ensuring continued innovation and competition throughout the marketplace. The CFPB should encourage market-driven solutions and avoid engaging in specific technical standard setting for consumer data sharing.

- Comprehensive Approach to Consumer Privacy and Transparency. Ensuring consumer privacy and transparency in how data is accessed, shared, and maintained should be central to the CFPB's process under Section 1033. The CFPB should clarify that the GLBA would apply to data aggregators and other authorized entities to ensure the appropriate consumer privacy standards and leverage existing GLBA disclosure obligations in place to protect customer information. The CFPB also should consider ways to improve the transparency of the consumer consent process, which would provide consumers with more awareness and control over their financial data. Additionally, the CFPB should consider promulgating specific disclosure requirements under Section 1032 of the Dodd-Frank Act, ensuring that data aggregators provide consumers with the information needed to make responsible decisions about the sharing of their information.

- Consistent Safeguarding of Consumer Data. The CFPB should ensure that data aggregators appropriately safeguard consumer data in a manner commensurate with the legal obligations placed on banks. The CFPB should clarify that GLBA applies to data aggregators for the purposes of consumer data security, and coordinate with the FTC to expand the Safeguards Rule to expressly address data aggregators' security practices. The CFPB should consider designating data aggregators as larger participants of the consumer financial data services marketplace, providing direct oversight over data aggregators through regular supervision and examination. The CFPB should also clarify the rights of consumers and the allocation of liability based on how the data flows between permissioned entities, beginning with clarifying liability for unauthorized transactions under Regulation E.

The rest of this letter elaborates on BPI's views regarding each of these important issues.

I. The CFPB's Efforts to Set Standards for Consumer Authorized Data Sharing Should Ensure Sufficient Flexibility and Innovation in the Marketplace.

BPI appreciates that the CFPB's actions to date related to consumer access to financial records have allowed the market to develop without direct regulatory intervention. The financial ecosystem has changed fundamentally since the enactment of Section 1033 of the Dodd-Frank Act over 10 years ago and, more so, since the CFPB released its Consumer Protection Principles on Consumer-Authorized Financial Data Sharing and Aggregation in 2017 (the "Principles").[3] Shifts in consumer demand for more digital and interactive financial products and services have dramatically changed the marketplace, which now includes an increasing number of fintechs and other companies facilitating access to consumer data to provide such products and services. This surge in adoption of digital products and services has accelerated banks' efforts to leverage market-developed technological solutions to help meet customer demand of banking outside the branch.

BPI believes a market driven approach is the best way to empower consumers to control their financial data while ensuring continued innovation in the marketplace. Under an industry-driven approach, participants are able to innovate and adapt more quickly to market chances and develop safer solutions to future issues. An overly prescriptive framework to implement Section 1033 will have the effect of limiting innovation and preventing solutions best determined by participants in this ecosystem. To that end, BPI recommends that any CFPB efforts pursuant to 1033 (or otherwise related to consumer authorized financial data sharing) continue to ensure sufficient flexibility and innovation in the marketplace.

A. The Financial Services Industry Continues to Advance the Consumer-Authorized Data Sharing Marketplace.

As discussed in the ANPR, consumer access to authorized data has increased the competition in provision of financial services to consumers. Banks are highly incentivized to facilitate consumer-authorized data access as a means of increasing consumer satisfaction and enhancing digital experience. 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, the below discussion provides recent technological advances and collaborations between banks, fintechs, and data aggregators that demonstrate how the industry has progressed the data sharing marketplace to better serve consumers.

First, 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.

Second, building on the advent of API-based data sharing, several banks have entered into data

[3] CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (October 18, 2017), available at cfpb_consumer-protection-principles_data-aggregation.pdf (consumerfinance.gov).

access agreements with aggregators to facilitate the data sharing process and dictate how data is accessed and protected.[4] Data access agreements are designed to establish contractual terms and operational processes in support of methods to safely and securely share financial data between banks and data aggregators, providing transparency between the parties as to how consumer data is shared. However, these agreements can be highly specific and tailored to meet the needs of the two parties and the nature of the access, and thus are not highly scalable or broadly applicable, resulting in a slow rate of migration from screen scraping and varying customer experiences. Most recently, The Clearing House released a Model Agreement template that banks, aggregators, and fintechs can use as a reference or foundation for entering into bilateral data access agreements.[5] Designed in consultation with banks and technology companies, this agreement demonstrates how the industry has worked together to ensure forward momentum for safe and secure consumer authorized data sharing practices.

Third, the financial services industry collectively has advanced the marketplace towards common technical standards for the secure access of consumer-permissioned data. For example, through the Financial Data Exchange ("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.[6] The broad adoption of FDX's API technical standard will improve security for the customer and create predictability for the industry. In addition to common technical standards, the industry is moving towards utilizing networks to facilitate access. For example, Akoya's Data Access Network facilitates direct connections utilizing FDX's API by providing a single point of integration for data providers and recipients and reducing the need for creating specific bilateral data access agreements.[7]

B. Industry-Led Standards Bodies are Best Positioned to Unify the Industry Around Common Technical Standards.

Industry-led standards bodies are best positioned to unify the financial industry around common and interoperable technical standards and to ensure rapid adaption to market innovations and changes in financial technology that would not be possible in a regulatory-led environment. Industry-led technical standards also can help maintain competition and innovation by reducing barriers to entry and providing a level playing field for market participants. By contrast, government-led technical standards may be less suitable to a broader set of market participants and more cumbersome to implement; moreover, development of such technical standards likely would be time-consuming, costly to develop, and unlikely to adapt quickly to market or technological changes.

Significant industry work already has been done to establish such technical standards. As noted above, FDX developed a common API that can facilitate secure data sharing among market participants. FDX continues to enhance its API specification by including new features and use cases for consumer-permissioned scenarios and has enhanced the data sharing ecosystem by developing user experience

[4] *See e.g.*, JP Morgan Chase, *"Plaid Signs Data Agreement with JP Morgan Chase"* (Oct. 22, 2018); *see also* TD Bank Group, *"TD enters into North American data-access agreement with Finicity"*, (Aug. 7, 2020); *see also* Envestnet, *"Wells Fargo and Envestnet | Yodlee Sign Data Exchange Agreement"*, (Sept. 24, 2020).

[5] *See* The Clearing House website at https://www.theclearinghouse.org/connected-banking/model-agreement.

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

[7] Press Release, "U.S. Bank and Akoya team up to accelerate safe, secure, and transparent consumer-permissioned financial data access", (Nov. 16, 2020); *see also* Akoya website at https://www.akoya.com/.

guidelines for the permissioning process and common data sharing terminology to align industry stakeholders.[8] With representation from market participants, FDX is uniquely situated to continue the development of technical standards for the industry.

BPI recommends that the CFPB avoid engaging in specific technical standard-setting work and, instead, consider methods by which it can encourage continued industry-led technical standard setting efforts in the consumer-permissioned data sharing marketplace. For example, in furthering these practices, the CFPB could consider how other market-driven solutions have been successful in establishing cross-industry standards (*e.g.*, Bluetooth, Mortgage Industry Standards Maintenance Organization ("MISMO"), Payment Card Industry Data Security Standard ("PCI DSS")).[9] By encouraging industry-led efforts, rather than setting specific technical standards, we believe the CFPB will allow for further innovation within the industry.

II. The CFPB Must Ensure a Comprehensive Approach to Consumer Privacy and Transparency to Increase Consumer Understanding of Data Use.

Despite various efforts to clarify how data is used once a consumer authorizes access,[10] there is significant room for improvement regarding transparency and consumer choice. Generally, consumers still are unaware that (1) depending on the circumstances, they are providing their credentials to a third-party data aggregator, rather than directly to a financial institution, and (2) their credentials or data could be further shared and/or used beyond their initial authorized access. In cases where data aggregators access consumer data through screen scraping or credential-based data access, banks are generally unable to ensure that the data corresponds to those fields for which the customer is authorizing access. Rather, in these instances, data aggregators can gain access to data attributes beyond those needed to provide the product or service requested by the consumer. These data attributes can have far reaching implications regarding a consumer's financial information, and can include, among other types of information, routing numbers, check images, demographic information, income details, email addresses, phone numbers, or IP addresses. Recent lawsuits indicate the increasing concerns related to potential violations of privacy because of the broad scope of this type of data access.[11]

One aspect of Section 1033 that may require further consideration by the CFPB as it relates to consumer privacy and transparency includes which data elements fall within a consumer's right of access. In this respect, the CFPB should carefully consider whether some form of standard is needed

---

[8] Press Release, *"Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5"* (December 8, 2020), available at https://financialdataexchange.org/FDX/News/Press-Releases/FDX_Launches_Open_Finance_Standards_And_FDX_API_4.5.aspx.

[9] For more information, refer to Bluetooth Specifications, MISMO Standards & Resources, and PCI DSS.

[10] See Bureau of Consumer Fin. Prot., Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18 2017) (2017 Principles) at 1, available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf. See 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/.

[11] For example, a recent class action lawsuit alleges Plaid potentially violating users' privacy by accessing customers' private data in violation of the California Consumer Protection Act ("CCPA"). https://www.courtlistener.com/docket/17361153/1/evans-v-plaid-inc/.

with respect to the types of data elements that can be shared with authorized entities and fourth parties and the corresponding standards applicable based on the sensitivity of the data. Regardless of the approach taken by the CFPB here, it is important that a careful, thoughtful approach is taken to ensure that all institutions provide a consistent type and amount of data regarding their customers. These considerations will help minimize privacy risks and allow consumers to better understand what kind of data is being accessed and used.

BPI fully supports consumers' ability to access their financial data and have control over the data they permission, and believes that when handled appropriately, access to data can benefit consumers. However, data access must occur in a secure, transparent manner that provides consumers with control and appropriate protections under relevant regulatory and legal frameworks.

A. Existing Privacy Laws Provide a Framework for Consumer Access to Financial Records Under Section 1033 of the Dodd-Frank Act.

Banks and other financial institutions have long been subject to comprehensive federal, state, and foreign standards related to the privacy and security of customer information. The need to protect the confidentiality and privacy of customer information has been deeply embedded in bank policies and operations for many years. Indeed, few other sectors have as extensive a set of legal and regulatory requirements that, together with industry standards, govern the collection, use, control, and transparency of customer data. These requirements include the GLBA and its implementing regulations, including Regulation P.

The GLBA standards require financial institutions to inform consumers about how their data is collected and shared and, in certain circumstances, to allow consumers to opt out of information sharing. The GLBA prescribes when customer information may be disclosed to nonaffiliated third parties and when financial institutions must allow customers an opportunity to opt out of information sharing. Further, banks' collection and use of personal information is subject to robust and thorough regulation and oversight at essentially every stage of the data lifecycle.

According to the Department of Treasury in a July 2018 report, data aggregators and consumer fintech application providers are subject to the GLBA.[12] However, it is not clear whether and how these entities comply with GLBA privacy standards, and no consistent method exists to supervise whether these firms appropriately comply with the standards set forth under the GLBA. To that end, it is imperative that the GLBA's privacy standards are applied consistently with respect to consumer authorized financial data sharing, regardless of the type of participant. BPI recommends the CFPB clarify that the GLBA applies to data aggregators and other authorized entities through the establishment of a direct "consumer" or "customer" relationship for the purposes of consumer privacy and ensure that such firms comply with these existing disclosure obligations.

Further, given that the GLBA and Section 1033 have overlapping but different goals with respect to consumers, it will be important for the CFPB to both consider and implement the two. For example, the GLBA privacy standards provide a broad definition of personal information that financial institutions must protect, including "personally identifiable financial information." By comparison, Section 1033

[12] U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation* (July 2018), https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

applies to information "concerning the consumer financial product or service" obtained from a covered entity, "including information relating to any transaction, series of transactions, or to the account including costs, charges, and usage data." In this context, the GLBA standards operate as a necessary floor with respect to how information should be protected, shared and the use disclosed in this context, but the CFPB also should ensure that those same principles are enhanced under the Section 1033 framework for all participants in the data sharing marketplace.

B. The CFPB Should Consider How to Enhance the Consumer Consent Process to Improve the Transparency of Data Access and Use.

Consumers should have full awareness over what information is shared, how it is shared, and to whom it is shared. Correspondingly, consumers must have the ability to grant consent to share their financial data for services or applications, and the fintechs or companies providing those services or applications, not the financial institution, should have the obligation to procure that consent. It is important to note that a bank or other financial institution is not authorizing the service, but rather is helping facilitate the request from the customer. Without the fourth party obtaining consent, the consumer could be confused about the party with which they are entering into an agreement and which party is holding their data.

Additionally, consumers should have the ability to confirm, modify, and revoke access once granted, and a clear and easy process to do so. The ability to confirm, modify, and revoke consent provides consumers with appropriate control over the data being accessed in order to protect themselves accordingly.

BPI applauds the CFPB for including control and informed consent as a key principle in its 2017 Principles.[13] The CFPB should consider working with the federal banking regulators and FTC to provide additional guidance on the informed consent principle. BPI also recommends, in building upon the Principles, that the CFPB consider ways to improve the transparency of the consent process and allow consumers to exercise control over the scope and duration of the data being obtained and used.

C. The CFPB Should Consider Promulgating Disclosure Requirements Under Section 1032 of the Dodd-Frank Act for Data Aggregators and Fintechs Accessing Consumer-Authorized Data.

Consumers cannot make informed choices and provide such consent without transparent, comprehensible, and readily accessible disclosures. To the extent that data use rights are not properly covered leveraging GLBA disclosure requirements, the CFPB also could consider exercising its authorities under Sections 1021(b)(1) and 1032 to promulgate disclosure requirements to ensure that consumers are provided with the information needed to make informed decisions about the sharing of their consumer financial data.[14] Section 1021(b)(1) of the Dodd-Frank Act requires the CFPB to ensure that "consumers are provided with timely and understandable information to make responsible decisions about their financial transactions."[15] Under Section 1032 of the Dodd-Frank Act, the CFPB can "prescribe rules to ensure that the features of any consumer financial product or service, both initially

[13] *See Principles, supra* note 3.

[14] 12 U.S.C. 5511(b)(1); 12 U.S.C. 5532.

[15] *Id.*

and over the term of the product or service, are fully, accurately, and effectively disclosed to consumers in a manner that permits consumers to understand the costs, benefits, and risks associated with the product or service, in light of the facts and circumstances."[16]

In implementing additional disclosure requirements for data aggregators, the CFPB should consider the following attributes in promulgating disclosure requirements:

- Disclosures should be clear and conspicuous, written in plain language, and presented in a simple format so that consumers can provide affirmative consent.
- Disclosures should include transparent information on what data is being accessed and obtained, and for what purposes.
- Disclosures should be harmonized across different jurisdictions and product categories. Where requirements cannot be harmonized, there must be guidance regarding which requirements take precedence.

In addition, the CFPB should consider providing a model disclosure to demonstrate the requirements of effective and informed consent. Through a model disclosure, the CFPB would achieve the dual goals of better informing and educating consumers about what to expect when consenting to access of their financial data, while also furthering consistency and clarity for market participants. As a part of this, the CFPB should strongly consider how best to place disclosure obligations on data aggregators and other authorized entities as it relates to the sharing, transfer, or sale of consumer financial data.

The CFPB should also consider whether the requirements for disclosures and obtaining affirmative consent should be recurring over time, providing consumers with more visibility into how their data is being used and the explicit opportunity to reassess data access. For example, the CFPB could require data aggregators to provide notices to consumers after a certain period of time indicating the terms of data use and providing consumers with the ability to revoke access.

The existing privacy regulations should also inform any potential model disclosure to ensure consistency and clarity in application for consumers and market participants, particularly as it may relate to the attributes articulated above.

III. The CFPB Should Ensure that Data Aggregators Appropriately Safeguard Consumer Data in a Manner Commensurate with the Legal Obligations Placed on Banks.

A. The CFPB Should Ensure that Data Aggregators Are Subject to Comprehensive Data Security Standards.

As previously discussed, banks are required to safeguard customer data and comply with strict regulatory requirements related to privacy and security. In addition to the disclosure obligations provided under the GLBA and Regulation P, financial institutions are required to appropriately safeguard customer data.[17] As a part of implementing the GLBA, the FTC set forth the Safeguards Rule, which

[16] 12 U.S.C. 5532.

[17] 15 U.S.C. § 6801.

requires financial institutions to assess and develop a documented security plan that describes company's programs to protect customer information.[18] Similarly, the federal banking agencies issued the Interagency Guidelines Establishing Information Security Standards ("Interagency Guidelines"), which requires banks to develop, implement, and maintain an information security program to identify and control risks to customer information and systems.[19] The Interagency Guidelines also require banks to perform regular risk assessments and conduct "appropriate due diligence" in selecting and monitoring service providers.[20] The federal banking agencies also issued the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Interagency Guidance") which outlines requirements relating to programs for incident response, including customer and regulator notification. To ensure compliance with this regulation and others, banks are regularly examined by prudential regulators.

The FTC has indicated that data aggregators and consumer fintech application providers significantly engaged in financial services and products are financial institutions under GLBA and therefore subject to the Safeguards Rule.[21] However, while the data security provisions of the GLBA are enforced by the federal banking agencies for depository institutions, and the SEC and CFTC for entities under their jurisdiction, the FTC does not have the authority to routinely supervise and examine institutions for compliance with GLBA provisions. Further, there is no federal standard for customer or regulator notification in the event of a data breach by a data aggregator.

Under the current framework, data aggregators access and store similar information to that of banks, but are not held to similar standards for safeguarding consumer data. Data aggregators security controls vary, as some firms may be limited by their size, resources, or compliance management systems to fully comply with the relevant privacy laws and these firms are not subject to regular supervision to ensure appropriate compliance. Without appropriate safeguards or oversight, data aggregators can pose potential risks to consumers related to unauthorized data access. For example, consumers face risks when they part with their banking credentials, which, when stolen, may enable identity theft or theft of funds. Additionally, without requirements for information security programs, the potential for a data breach at a data aggregator may result in misuse of customer data.

BPI recommends that the CFPB, alongside the other relevant agencies, clarify that data aggregators, as financial institutions, should implement similar standards as those provided under the FTC's Safeguards Rule, the Interagency Guidelines and the Interagency Guidance. As such, BPI recommends that the CFPB coordinate with the FTC, and others as appropriate, to expand the Safeguards Rule and guidance to expressly address the activities of data aggregators. Reducing the disparity in data security expectations and practices between banks and data aggregators will help ensure that consumer financial data is being protected and handled appropriately.

---

[18] 16 C.F.R. pt. 314. The SEC similarly has promulgated a rule for those entities subject to its jurisdiction, pursuant to Regulation S-P. 17 C.F.R. 243.30.

[19] 12 C.F.R. pt. 30, App. B.

[20] 12 C.F.R. pt. 30, App. B, III D.

[21] Federal Trade Commission, Financial Institutions and Customer Information: Complying with the Safeguards Rule (Apr. 2006), available at: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutionscustomer-information-complying (stating that the Safeguards Rule applies to companies that receive information about the customers of other financial institutions).

B. The CFPB Should Consider Designating Data Aggregators as Larger Participants of the Consumer Financial Data Services Marketplace.

Pursuant to Section 1024 of the Dodd-Frank Act, the CFPB has authority over "any covered person who… is a larger participant of a market for other consumer financial products or services, as defined by rule."[22] To date, the CFPB has defined "larger participants" in the consumer reporting, consumer debt collection, student loan servicing, international money transfer, and automobile financing markets, which has allowed the agency to examine the activities of these larger participants in a similar manner to those covered persons routinely supervised by the CFPB pursuant to Section 1025.[23]

BPI recommends that the CFPB use its authority under Section 1024 to engage in a larger participant rulemaking in order to supervise the activities of data aggregators and other similar firms. As a general matter, and as denoted throughout this letter, there is a clear gap in oversight for these firms and their activities. Data aggregators hold an enormous volume of consumer financial data that has the potential to impact millions of consumers. Further, the bulk of data processing is managed by a small group of large companies. For example, one large data aggregator connects to 200 million consumer bank accounts across 11,000 U.S. banks.[24] Considering the volume of data accessed and held by data aggregators and corresponding potential risks to consumers, engaging in such a rulemaking would be appropriate and in the best interest to consumers.

C. The CFPB Should Clarify the Rights of Consumers and Liability in the Event of Unauthorized Transfers and Fraudulent Activity.

The sharing of financial data between permissioned entities increases the potential for unauthorized transfers and fraudulent activity. In prepared remarks from September 2019, FinCEN Director Kenneth Blanco warned that cybercriminals appear to be using data aggregators to facilitate account takeovers and create fraudulent accounts as part of identity theft or synthetic identify fraud.[25] Consumers may not be aware that by providing fintechs access to their financial data, they shift liability for loss protections to another entity. Further, considering data aggregators collect and store significant amounts of customer data, they pose greater potential for a cyber breach. Consumers generally turn to their banks whenever a data breach or unauthorized account transaction occurs, even if the bank was not responsible for the incident. While banks support consumer access to their financial records and are highly incentivized to facilitate that access, banks should not be held accountable for the actions of fintech services after providing authorized access to that data. Additionally, to facilitate access, banks incur significant financial and operational costs to ensure consumers' sensitive financial data is shared in a safe and secure manner. The current arrangement leaves the financial, operational, and reputational risks with the bank and limited liability or accountability with data aggregators.

---

[22] 12 U.S.C. §5514 (a)(1)(B).

[23] 12 C.F.R. 1090.

[24] Press Release *"Justice Department Sues to Block Visa's Proposed Acquisition of Plaid"*, (November 5, 2020), *available at* https://www.justice.gov/opa/pr/justice-department-sues-block-visas-proposed-acquisition-plaid.

[25] 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

BPI believes that liability for ensuring appropriate consumer protections should attach to the flow of the data. To that end, we recommend that the CFPB clarify the allocation of liability when data is shared between permissioned entities. An initial step the CFPB could take is by clarifying the allocation of liability for unauthorized transactions under Regulation E. Regulation E, which implements the Electronic Fund Transfer Act, "establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer and remittance transfer services and of financial institutions or other persons that offer these services."[26] While existing federal statutes such as Regulation E and GLBA make clear the rights, roles, protections, and responsibilities associated with fraud, unauthorized transactions, and breaches of data security for financial institutions and their customers, it is not clear how and under what circumstances the involvement of a third-party data aggregator in the offending transaction impacts the customer's liability for any losses incurred. Specifically, BPI recommends the CFPB clarify the following:

- Whether a single sign-on service provided by a data aggregator constitutes an "access device" because it is a "code, or other means of access to a consumer's account";

- Whether a data aggregator is a "financial institution" because it "issues an access device and agrees with a consumer to provide electronic fund transfer services" by providing consumers a single sign-on service and permitting the initiation of electronic funds transfers through the bank; or

- Whether data aggregator is a "service provider" to the consumer for purposes of Section 1005.14, and therefore subject to liability for unauthorized transfers pursuant to Comment 14(b)-1, if it does not have an agreement with the bank regarding specific access (*i.e.*, outside the scope of any services it may provide to or on behalf of the bank).

As previously noted, some banks and data aggregators have entered into bilateral data access agreements that dictate how data is accessed and protected through APIs, conditioned on contractual liability and indemnification of the bank. Nevertheless, by clarifying liability when data is shared across permissioned entities, the CFPB will provide consumers with more transparency into which party is liable for unauthorized transactions or potentially fraudulent activity and empower consumers to control authorizing access to their data. Clarifying liability also would encourage all market participants to ensure they have appropriate security controls and safeguards in place to protect consumer data.

IV. Conclusion.

BPI appreciates the CFPB's continued engagement on the topic of consumer access to financial records under Section 1033 of the Dodd-Frank Act. We believe permissioned access to financial data will play an increasingly important role in the future of financial services. BPI recommends the CFPB continue to work with the financial services industry, consumers, and regulatory stakeholders to guide implementation of Section 1033 and ensure appropriate consumer protections within the data sharing marketplace.

[26] 12 C.F.R. §1005.1(b).

* * * * *

Thank you for the opportunity to comment on the Section 1033 ANPR. If you have any questions, please contact, Stephanie Wake at (202) 589-2432 or by email at Stephanie.Wake@bpi.com, or Naeha Prakash at (202) 589-2429 or by email at Naeha.Prakash@bpi.com.

Respectfully submitted,

Naeha Prakash
Senior Vice President & Associate General Counsel for
Consumer Regulatory Affairs
Bank Policy Institute