December 29, 2023

Via Electronic Mail

Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20052
2023-NPRM-Data-Rights@cfpb.gov

Re: Docket No. CFPB-2023-0052 – Required Rulemaking on Personal Financial Data Rights

To Whom it May Concern:

The Consumer Bankers Association (CBA)[1] appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (the Bureau) Notice of Proposed Rulemaking on Personal Financial Data Rights[2] (the NPRM) pursuant to Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).[3] CBA appreciates the work that the Bureau has done over the years in connection with Section 1033. This NPRM represents another step toward enhancing consumer access to their data, but the proposal has several concerns that must be addressed before finalization.

CBA is concerned by the NPRM's general trend toward shifting many costs and responsibilities, including the monitoring of certain market participant behavior, onto data providers. The Bureau should undertake the responsibilities or distribute these costs and responsibilities more equitably across stakeholders in the open banking ecosystem the Bureau is creating. This approach is surprising given how other open banking jurisdictions have addressed these issues, such as the allocation of liability. For instance, among other concerns, the NPRM appears to envision the Bureau playing a startlingly smaller role than the Bureau typically would in the supervision of market participants for compliance with Federal consumer financial laws. CBA advises the Bureau to reexamine several of the technical details of the rulemaking – such as the scope of coverage, elements of the data to be shared, and expectations for third parties – to better achieve the Bureau's stated goal of enhancing consumer access to their data. In light of the breadth, complexity, and importance of the suggested changes to ensure a

[1] CBA is the only national trade association focused exclusively on retail banking. Established in 1919, the association is a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly $3 trillion in consumer loans, and provide $270 billion in small business loans.
[2] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796 (Oct. 31, 2023).
[3] 12 U.S.C. § 5533.

durable, efficient, and practicable Section 1033 final rule, CBA requests to meet with the Bureau to explore solutions to the issues outlined in this letter.

CBA recommends the Bureau take the following actions to better protect consumers and appropriately address industry concerns about the feasibility, durability, and quality of the Section 1033 final rule:

- Data Providers
  - *Scope of Covered Data Providers is Too Narrow*
    - Adopt a broad scope of coverage for not just asset accounts, but also for credit products, like captive auto loan accounts, and non-bank credit alternatives, like Buy Now Pay Later (BNPL) Products and Electronic Benefit Transfer (EBT) Cards.
  - *Fees*
    - Allow data providers to charge reasonable and proportional fees to authorized third parties, or data aggregators acting on behalf of third parties, accessing the developer interface.
  - *Frequency of Access*
    - Clarify what makes an access cap "unreasonable."
    - Declare it is reasonable for a data provider to limit an authorized third party's or data aggregator's access if there is a risk the authorized third party's or data aggregator's repeated access attempts may cause unreasonable technical strain on the data provider's system or hinder the ability of other authorized third parties and data aggregators to access the developer interface.
  - *Authorization and Authentication*
    - Affirm data providers' right, but not obligation, to confirm a third party has followed the authorization procedures.
    - Permit, but do not require, data providers to confirm additional aspects of the scope of authorization as may be reasonably necessary and appropriate.
    - Clarify that a revocation method being "reasonable" does not limit a data provider's ability to provide clear disclosures about data access to their consumers.
    - Allow consumers to modify the scope of an authorized third party's authorization without needing to terminate the authorization entirely.
    - Review authorizations as part of the Bureau's supervision of third parties and data aggregators.
  - *Conditions of Access*
    - Specify that denying a third party access to a developer interface based on guidance issued by prudential regulators with respect to third party risk management is a reasonable denial.

- Covered Data
  - *Transaction Information*
    - Require data providers to share only transaction information they already retain and explicitly acknowledge that data providers are not required to retain any new records about a consumer.
    - Obligate data providers to make 12 months, rather than 24 months, of historical transaction information available.
    - Do not mandate data providers share reward credits per transaction.
  - *Account Balance*
    - Provide additional examples of "account balance" to assist data providers in complying with the final rule.
  - *Information to Initiate a Transaction to or from a Regulation E Account*
    - Do not mandate sharing information to initiate payment to or from a Regulation E account.
    - To the extent information to initiate payment to or from a Regulation E account is required to be shared by data providers, place appropriate liability obligations on third parties in recognition of the increased liability risk that data providers will face.
  - *Terms and Conditions*
    - Only require a disclosure of a narrow set of discrete data elements – such as standard annual percentage rate (APR) or annual percentage yield (APY) – as part of making "terms and conditions" available.
    - Require sharing of realized fees, rather than the applicable fee schedule.
    - Do not require sharing of rewards program terms, whether a consumer has opted into overdraft coverage, and whether the consumer has entered into an arbitration agreement.
  - *Upcoming Bill Information*
    - Exclude third party bill payments that have been scheduled through the data provider from being shared.
  - *Basic Account Verification Information*
    - Maintain the NPRM's narrow scope of basic account information category to name, address, email address, and phone number.
- Screen Scraping
  - Expressly prohibit the use of screen scraping by third parties and data aggregators of any data made available through a developer interface, not just covered data.
  - Shift the obligation away from banks and to the Bureau itself to supervise, assess, and pursue enforcement actions against third parties and data aggregators that improperly engage in screen scraping, or other violations of Federal consumer financial laws.
- Developer Interfaces
  - Acknowledge a standard-setting organization (SSO), rather than the Bureau, should set what is commercially reasonable for a developer interface, which may vary by use case.

- Third Parties & Data Aggregators
  - *Authorization Disclosures*
    - Require disclosure of complaint/dispute contact information for the third party and data aggregator (if applicable) as part of authorization disclosure.
  - *Certification Statement*
    - Require third parties certify they will comply with third party obligations for all data accessed through a developer interface, rather than just covered data.
    - Mandate third parties certify their acceptance of liability in certain circumstances, and that they are adequately capitalized and carry sufficient indemnity insurance to fulfill their liability obligations.
  - *Servicing or Processing*
    - Provide a non-exhaustive list of activities that constitute permissible "servicing or processing."
  - *Secondary Use Prohibitions*
    - Prohibit reverse engineering confidential, proprietary information or other trade secrets.
    - Include definitions of "targeted advertising," "cross-selling of other products or services," "sale of covered data," and "consumer's requested product or service."
  - *Gramm-Leach-Bliley Act (GLBA)[4] Obligations*
    - Clarify whether, and to what extent, the data use limitations contained in a Section 1033 final rule supersede any limitations that might exist on the use of that data under GLBA.
- SSOs
  - Revise the "openness" and "balance" prongs of the SSO-recognition process to acknowledge that data access ecosystem participants electing to not join an SSO does not mean that such SSO lacks "openness" or "balance."
  - Revise the "due process" and "transparency" prongs of the SSO-recognition process to protect anonymity of participant viewpoints and encourage open dialogue.
  - Treat compliance with an SSO's promulgated standards as sufficient, but not necessary, to establish compliance with the Section 1033 final rule.
- Liability
  - Explicitly state liability rests with the responsible third party or data aggregator if a consumer's credentials are misused to initiate a fraudulent transaction by such party or are impermissibly acquired by another actor through a data breach the party experienced.
  - Mandate third parties and data aggregators be adequately capitalized and carry sufficient indemnity insurance to satisfy liability obligations.
  - Obligate third parties to certify as part of the certification statement that they are adequately capitalized, have accepted their liability obligations, and are carrying sufficient indemnity insurance.

[4] Public Law 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. 6801 *et seq.*).

- Compliance Timeframes
    - Adopt a two-track compliance timeline based on whether the Bureau has recognized a standard-setting body as an issuer of qualified industry standard.
        - If the Bureau has recognized at least one standard-setting body, then the largest data providers should have a minimum of 12 months to come into compliance.
        - If the Bureau has not recognized at least one standard-setting body, then the largest data providers should have a minimum of 24 months to come into compliance.
- Additional Matters
    - Clarify whether virtual currencies are "funds" for purposes of determining whether nonbanks offering virtual currencies fall within the scope of "data providers."
    - State that a data provider complying with obligations under the Section 1033 final rule does not make that data provider a "furnisher" under the Fair Credit Reporting Act (FCRA).[5]
    - Provide further information on how the obligations under the Section 1033 final rule intersect with those under the Bureau's Advisory Opinion on Consumer Information Requests to Large Banks and Credit Unions (1034(c) AO).[6]
    - Identify what exact activities, if undertaken, would result in a data aggregator being classified as a "consumer reporting agency" under the FCRA.

A robust discussion of each of the foregoing matters is below.

I. Preliminary Concerns

A. Pursuing a Section 1033 Rulemaking to Enhance Competition in the Market is an Inadequate Justification because the Consumer Credit Card and Deposit Account Markets are Already Very Competitive

CBA supports the underlying principles of open banking and how it may enhance consumer experiences, but is deeply concerned by the Bureau's inaccurate assertion that the Section 1033 rulemaking, and open banking in general, are necessary to increase competition in the marketplace. The Bureau should avoid perpetuating these inaccurate claims in its promulgation of the Section 1033 final rule and any accompanying press releases, speeches, or blog posts. The Bureau asserts throughout the NPRM that "commercial actors are able to use their market power and incumbency to privilege their concerns and interests above fair competition that could benefit consumers."[7] Director

[5] 15 U.S.C. 1681 *et seq*. (implemented by Regulation V, 12 C.F.R. § 1022).
[6] Consumer Information Requests to Large Banks and Credit Unions, 88 Fed. Reg. 71279 (Oct. 16, 2023).
[7] Rohit Chopra, Dir., Consumer Fin. Prot. Bureau, *Prepared Remarks of CFPB Director Rohit Chopra on the Proposed Personal Financial Data Rights Rule* (Oct. 19, 2023),

Chopra's remarks introducing the NPRM magnify this inaccurate rhetoric, describing consumer finance markets as "structured in ways that don't allow consumers to exercise their power"[8] and asserting that in credit cards and deposit accounts markets "financial firms have learned that they don't need to provide great rates or customer service for a sustained period of time. Instead, they can attract customers with teaser rates, change them whenever they want, and make it bureaucratically difficult to switch."[9] Director Chopra further summarized that a Section 1033 rule "would help address many of the root causes of sticky banking – by giving people more power to walk away from bad service and enabling small community banks and nascent competitors to peel away customers through better products and services with more favorable rates."[10]

CBA strongly objects to the assertion that consumer credit card and deposit accounts markets are not competitive, as well as the misleading claim that banks and credit card issuers do not already provide stellar service to their customers. With respect to the financial services industry as a whole, the United States has one of the largest, most diverse, and most competitive financial industries in the world, especially compared to other advanced economies, like Canada, that have highly concentrated and coordinated banking markets.[11] Additionally, the financial services industry in the United States is far less concentrated and far more competitive than other consumer-facing industry sectors when examining the share of total sales captured by the top four firms in each industry on a national basis.[12] The United States also has a significantly greater number of banks than other markets. For example, while there are only 28 domestic banks in Canada, in the U.S. that number exceeds 7,000.[13]

Consumer credit card and deposit account markets specifically are highly competitive within the already competitive broad financial services sector. Despite how the Bureau characterizes the findings of the October 2023 CARD Act Report[14] in its press release,[15]

---

https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-the-proposed-personal-financial-data-rights-rule/.

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] Lawrence Pruss, *The Differences Between Banking in the US and Canada*, FIN. BRAND (Oct. 2, 2015), https://thefinancialbrand.com/54467/comparing-united-states-canadian-banking-systems/.

[12] Francisco Covas & Paul Calem, *Five Important Facts about the Competitiveness of the U.S. Banking Industry*, BANK POL'Y INST. (Feb. 24, 2022), https://bpi.com/five-important-facts-about-the-competitiveness-of-the-u-s-banking-industry/.

[13] Pruss, *supra* note 11.

[14] Consumer Financial Protection Bureau, *The Consumer Credit Card Market* 18 (2023) [hereinafter *2023 CARD Act Report*], https://files.consumerfinance.gov/f/documents/cfpb_consumer-credit-card-market-report_2023.pdf.

[15] *See* Consumer Financial Protection Bureau, *CFPB Report Finds Credit Card Companies Charged Consumers Record-High $130 Billion in Interest and Fees in 2022* (Oct. 25, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-report-finds-credit-card-companies-charged-consumers-record-high-130-billion-in-interest-and-fees-in-2022/ ("Major credit card companies' profits are now higher than pre-pandemic levels, potentially signaling a lack of competition in a market consistently dominated by the top 10 credit card companies").

the October 2023 CARD Act Report itself clearly states that the market shares of the top ten credit card issuers declined by 4% from 2016 to 2022,[16] whereas market share for the next 20 issuers grew by the same percentage in that time frame,[17] clearly demonstrating that the largest credit card companies are losing market share to smaller banks, a sign of a competitive market. Credit card issuers continue to compete intensively to win new customers, demonstrated by the fact that in 2022 credit card marketing efforts were at their highest since at least 2015.[18] Continuing innovations in the credit card market, such as soft credit inquiries, place more credit card offers in front of consumers while simultaneously benefitting their financial well-being.[19] The competition amongst card issuers is highlighted by the fact that there were $53 billion in balance transfers in 2022,[20] demonstrating that a significant amount of credit card loans are moving from one card issuer to another. Even after a credit card issuer "wins" a consumer, the issuer still needs to fight to keep that consumer's business, as consumers have multiple credit card options to select from when making a purchase. The October 2023 CARD Act Report summarizes that,

> "[s]ince consumers often carry more than one credit card, credit card issuers compete to acquire and retain 'top of wallet' status as consumers' primary method of payment. Issuers must refresh product offerings and provide new benefits regularly to ensure cardholders reach for their product first at checkout or keep their card as the default option in a mobile wallet. Issuers depend on their card being consumers' top-of-wallet card to maintain interchange revenue, grow interest-incurring balances, and gain marketable insights on consumer spending."[21]

Competition in the deposit account market is likewise fiercely competitive. Fourteen percent of American consumers opened new checking accounts by the summer of

---

[16] *2023 CARD Act Report*, *supra* note 14, at 18.
[17] *Id.* at 19, fig. 3.
[18] *Id.* at p. 74.
[19] *Id.* at 162-63. ("During a typical credit card application process, the applicant provides the issuer with personal information that enables the issuer to check the applicant's credit history with one or more consumer reporting agencies. The consumer reporting agency then records the credit inquiry on the applicant's credit report, regardless of whether the applicant is ultimately approved by the issuer. These "hard" credit inquiries on the applicant's credit report can lower consumer credit scores, all else being equal.... For many borrowers, the use of soft credit inquiries alters the credit card shopping and application process. For borrowers in the shopping process who are unsure of their qualifications, the use of soft inquiries may encourage such borrowers to check their eligibility for a card with better terms rather than applying only for cards for which they may be more likely to qualify. Borrowers who are not approved following a soft pull can move on to the next card application with less concern that the denial has affected their credit score or reduced their likelihood of approval for their next card.").
[20] *Id.* at 163. ("Depending on the duration of the promotion and the interest rate differential, as well as the consumer's repayment behavior, savings from balance transfers can be significantly higher than the upfront cost of the initial balance transfer fee.").
[21] *Id.* at 88, fig. 18.

2023,[22] a rate that grows higher each year.[23] Further, nearly half of new checking accounts in 2023 were with digital banks or fintechs.[24] Additional financial market data and reporting shows that competition among institutions for deposits is robust, with banks experiencing increased pressure to offer competitive deposit rates and services to attract new customers.[25] Indeed, it is this robust competition in the market that has led to innovative developments in deposit products including more flexible overdraft plans,[26] adoption of peer-to-peer payment platforms, and enhanced mobile application features.

The claim that banks and credit card issuers do not already provide stellar service to their customers is similarly untenable and not evidenced by consumer sentiment. For example, when asked why they keep their checking accounts, 40% *more* consumers cite satisfaction with good customer service than the inconvenience of switching.[27] Banking services are increasingly provided through multiple platforms – digital, telephone, and other non-brick-and-mortar tools – providing consumers more convenience. The retail banking industry has been cited as a case study on how to improve engagement and deliver superior customer experiences,[28] a description that does not align with the Bureau's mischaracterization of the industry. Polling data further reinforces consumer satisfaction with the service provided by their bank. For example, a February 2022 ABA/Morning Consult Survey found that 9 in 10 Americans with a bank account (89%) say they are "very satisfied" or "satisfied" with their primary bank, and 88% agree they

---

[22] *See* Ron Shevlin, FORBES, *How Fintechs Are Dominating New Checking Account Openings* (Jul. 5, 2023), https://www.forbes.com/sites/ronshevlin/2023/07/05/the-checking-account-war-is-over-and-the-fintechs-have-won/?sh=888432a3a310 .

[23] Ten percent of consumers opened a new checking account in 2020. Twelve percent of consumers opened a new checking account in 2021. Fifteen percent of consumers opened a new checking account in 2022. *See id.*

[24] *See id.*

[25] *See* Alex Graf & Syed Muhammad Ghaznavi, S&P Global, *Banks leverage high-cost products to attract deposits as competition intensifies* (Jun. 27, 2023), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/banks-leverage-high-cost-products-to-attract-deposits-as-competition-intensifies-76215128; *see also* Nathan Stovall & Xylex Mangulabnan, S&P Global, *Bank margins slide as deposit costs charge higher* (Aug. 30, 2023), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/bank-margins-slide-as-deposit-costs-charge-higher-77250072.

[26] Consumer Financial Protection Bureau, *Overdraft/NSF metrics for Top 20 banks based on overdraft/NSF revenue reported* (Feb. 10, 2022), https://files.consumerfinance.gov/f/documents/cfpb_overdraft-chart_2022-02.pdf.

[27] Mary Wisniewski, Bankrate, *Survey: Consumers stick with the same checking account for an average of 17 years* (Jan. 4, 2022), https://www.bankrate.com/banking/how-long-people-keep-their-checking-savings-accounts/.

[28] *U.S. Retail Banks Nail Transition to Digital during Pandemic, J.D. Power Finds*, J.D. Power (April 27, 2021), https://www.jdpower.com/business/press-releases/2021-us-retail-banking-satisfaction-study. ("If you're looking for a case study in how to improve engagement and deliver a superior customer experience in the face of massive disruption, look no further than the U.S. retail banking industry's response to the COVID-19 pandemic . . . The fact that satisfaction has improved most among customers who say they feel worse off financially speaks volumes to the proactive efforts many banks launched to support their customers in a period of heightened financial stress.") (quoting Paul McAdam, senior director, banking intelligence at J.D. Power).

have multiple options when selecting products and services such as bank accounts, loans, and credit cards.[29] The Bureau's own 2021 Consumer Response Annual Report found that when a consumer had a complaint about the service provided by a financial institution, banks and other companies "overwhelmingly met the timeliness expectation in their responses."[30] Industry has shared with the Bureau information about how it provides stellar customer service,[31] yet the Bureau still asserts in the NPRM that "[w]hen a consumer can switch with less friction, this will create incentives for superior customer service and more favorable terms."[32] CBA urges the Bureau to avoid relying on mischaracterizations of already-competitive markets to unnecessarily support its required rulemaking objectives, and instead rely on the facts to fulfill its rulemaking requirements.

B. There is a Question Whether the Bureau has the Statutory Authority under Section 1033 for the Proposals Contained in the NPRM

Under Section 1033, covered persons are required to "*make available to a consumer, upon request*, information in the control or possession of the covered person… including *information relating to any transaction*, series of transactions, or to the account *including costs, charges and usage data*."[33] Such information is to "be made available *in an electronic form usable by consumers*."[34] This plain statutory language is fundamentally centered on a consumer's right to access their own information; in fact, the title of Section 1033 is "[c]onsumer rights to access information."[35] The statutory language says nothing about the ability "for individuals to fire, or walk away from, their financial provider for whatever reason"[36] in connection with only deposit accounts or credit card accounts. The statute also makes no reference to fees, SSOs, application programming interfaces (APIs), or other fundamental aspects of the NPRM. The language contained in Section 1033 is clearly focused on consumer access to their own

---

[29] *See, e.g.*, American Bankers Association, ABA Unveils New Consumer Polling Data on Major Bank Policy Issues at 2022 Washington Summit (Mar. 8, 2022), https://www.aba.com/about-us/press-room/press-releases/aba-unveils-new-consumer-polling-data-on-major-bank-policy-issues-at-2022-washington-summit. In addition, 48% of consumers trust banks the most to keep their information secure, compared to the only 13% of consumers who trust non-bank payment providers to keep their information secure. American Bankers Association, Consumer Bank Satisfaction Infographic (Oct. 15, 2021), https://www.aba.com/news-research/research-analysis/consumer-bank-satisfaction.

[30] Consumer Financial Protection Bureau, Consumer Response Annual Report for 2021, at 17 (2022), https://files.consumerfinance.gov/f/documents/cfpb_2021-consumer-response-annual-report_2022-03.pdf.

[31] *See, e.g.*, Bank Pol'y Inst. et al., *Comments in Response to Request for Information Regarding Relationship Banking and Customer Service, Docket No. CFPB-2022-0040* (Aug. 22, 2022), https://www.consumerbankers.com/sites/default/files/Joint_Comment_CFPB_CustServRFI_8.22.22.pdf

[32] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796(Oct. 31, 2023).

[33] 12 U.S.C. § 5533(a).

[34] 12 U.S.C. § 5533(a).

[35] 12 U.S.C. § 5533.

[36] Rohit Chopra, Dir., Consumer Fin. Prot. Bureau, *Prepared Remarks at Money 20/20* (Oct. 25, 2022), https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/.

information and not reshaping financial markets in a way that will have vast economic and political significance[37] as "[a] more decentralized and neutral consumer financial market structure [which] has the potential to reshape how companies compete in the sphere."[38] If Congress intended to create an open banking ecosystem similar to those in other jurisdictions, Congress would have clearly done so.

In the NPRM's discussion of the Bureau's legal authority, the Bureau asserts that the foregoing language grants it the authority "to establish a framework that readily makes available covered data in an electronic form usable by consumers and third parties acting on behalf of consumers,"[39] as well as "authority to specify procedures to ensure third parties are truly acting on behalf of consumers when accessing covered data."[40] However, it is not clear that the language of Section 1033 – which is centered on making information available to consumers in an electronic form – grants the Bureau the authority to dictate the creation and attributes of an entire data access ecosystem for data holders, consumers, third parties, and data aggregators in the name of facilitating open banking, in addition to the authority to limit fees in this ecosystem and create an SSO recognition regime. There is also a major question as to whether Congress intended to impart such a dramatic mandate, including potential impacts to safe and sound banking practices, to the Bureau through this straightforward, and relatively brief, language regarding consumer access to information.

C. The Bureau Considers the Activities of Other Open Banking Jurisdictions When Convenient, But Has Deviated from These Jurisdictions' Approaches in Significant Ways Without Sufficient Justification, Resulting in Open Questions for Industry that Are Not Answered in the NPRM

Regulators and many market participants may agree on the importance of open banking, but there is a valid question as to whether open banking should be implemented by stretching statutory text to justify the creation of an open banking environment through regulation, as opposed to implementing open banking through legislation or based on natural developments in a competitive market. The NPRM points to the implementation of open banking in other jurisdictions such as Australia and the United Kingdom multiple times,[41] yet these open banking initiatives were not implemented in the same manner as the Bureau is attempting in the United States. For example, open banking in the United Kingdom was introduced through a legislative mandate. In 2015, the European Union introduced the Revised Payment Services Directive (PSD2),[42] which repealed and replaced the Payment Services Directive

---

[37] *Cf. West Virginia v. Environmental Protection Agency*, 597 U.S. ___ (2022).
[38] Rohit Chopra, Dir., Consumer Fin. Prot. Bureau, *Prepared Remarks at Money 20/20* (Oct. 25, 2022), https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/.
[39] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. at 74802
[40] *Id.*
[41] *See, e.g.*, *id.* at 74816.
[42] Directive 2015/2366/EU of the European Parliament and of the Council (Nov. 25, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

(PSD1).[43] PSD2 generally sets out a regulatory regime for providers of payment services, restricts the provision of payment services as a regular business to certain types of entities, and requires the authorization or registration of providers of payment services which do not otherwise have the status of payment service provider. PSD2 was transposed into United Kingdom legislation by the Treasury in the Payment Services Regulations 2017,[44] which designated the Financial Conduct Authority (FCA) as the competent authority for PSD2.[45] The FCA subsequently published a PSD2 policy statement[46] and approach document[47] relating to implementation of PSD2. In contrast to the Bureau's murky authority to attempt to introduce open banking based on Section 1033's requirement to facilitate consumer access to data in an electronic format, the authority for implementation of an open banking regime, and the FCA's authority to supervise and manage open banking efforts, was clearly delineated and outlined in the United Kingdom. In addition to ensuring that regulation appropriately reflects Congressional intent, the existence of clear authority is vital for ensuring the continued durability, as well as effective implementation, of an open banking framework. The Bureau should meaningfully evaluate whether its authority under Section 1033 is truly sufficient for effectuating open banking.

These other jurisdictions generally have a more robust, holistic approach to open banking, several important elements of which the Bureau has either just not incorporated or significantly deviated from. For example, as further discussed in Part VIII, these jurisdictions allocate liability among the parties of the data access ecosystem by requiring third parties to take on liability obligations and maintain indemnity insurance. The Bureau in the NPRM has failed to meaningfully address liability or insurance in such a manner. Moreover, even these more robust approaches are continually being reevaluated and added to. For example, in June 2022 the European Banking Authority submitted a reply to the European Commission with technical advice on PSD2, offering specific, tailored feedback on scope and definitions, rights and obligations, customer authentication, and enforcement.[48] If the Bureau intends to look

---

[43] Directive 2007/64/EC of the European Parliament and of the Council (Nov. 13, 2007), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32007L0064#:~:text=Directive%202007%2F64%2FEC%20-of%20the%20European%20Parliament%20and%20of,and%20repealing%20Directive%2097%2F5%2FEC%20%28Text%20with%20EEA%20relevance%29.

[44] The Payment Services Regulations 2017(SI 2017/752), https://www.legislation.gov.uk/uksi/2017/752/pdfs/uksi_20170752_en.pdf.

[45] *Id.*

[46] Financial Conduct Authority, *Policy Statement PS17/19 – Implementation of the revised Payment Services Directive (PSD2): Approach Document and final Handbook changes* (Sept. 2017), https://www.fca.org.uk/publication/policy/ps17-19.pdf.

[47] Financial Conduct Authority, *Payment Services and Electronic Money – Our Approach: The FCA's role under the Payment Service Regulations 2017 and the Electronic Money Regulations 2011* (Nov. 2021, originally published Sept. 2017), https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.

[48] *See* European Banking Authority, *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)* (Jun. 23, 2022), https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/20

to the implementation of open banking in other jurisdictions for inspiration, then the Bureau should take care to address the pain points that other jurisdictions have experienced and identified, and learn from ongoing developments in those jurisdictions rather than a piecemeal approach that leaves data providers in significantly worse positions and tilting competitive markets while increasing consumer risk.

D. The Bureau's Cost-Benefit Analysis is Deficient and Severely Underestimates Costs to Industry

The NPRM's cost-benefit analysis severely underestimates the costs that will be faced by market participants. The Bureau particularly misjudges the costs that data providers will face in building out the new data access ecosystem. As summarized in Part II.B, data providers will be obligated to fund the creation of developer interfaces, many aspects of which have not yet been fully defined or clarified. New systems will need to be developed to retain and share data that many data providers may not currently share, or share existing data in new ways that, to date, are not beneficial. Data providers would face additional costs under the NPRM for monitoring the compliance, consistent with existing prudential regulatory expectations, of all other parties in the ecosystem. The proposal also contemplates differing performance standards depending on the size of the institution, but this approach increases costs to larger covered data providers without providing any benefit, as any authorized third party will have to design systems capable of ingesting data from the slowest permitted data provider. These obligations would be in addition to the pre-existing risk management and fraud prevention obligations many data providers face due to the vastness in which the potential universe of third parties could be expanded to, including those well beyond other financial service providers. Data providers would also need to create, operate, and continuously improve these systems, including systems to detect and defend against constantly evolving cyber threats. The net result is that more human and technical resources will be needed to manage access by third parties and data aggregators.

II. Data Providers

A. Scope of Covered Data Providers is Too Narrow

The Bureau should adopt a broad scope of coverage for not just asset accounts, but also for credit products, like captive auto loan accounts, and non-bank credit alternatives, like BNPL Products and EBT Cards.

The scope of data providers covered by the rule remains too narrow, so before issuing the Section 1033 final rule the Bureau should expand the scope of data providers in a manner consistent with the Administrative Procedures Act (APA)[49] rulemaking process. This expansion can be done consistent with the APA rulemaking process by proposing

22/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.

[49] Public Law 79–404, 60 Stat. 237.

an additional rule to expand the scope of data providers. The NPRM proposes to cover data providers controlling or possessing covered data concerning "Regulation E asset accounts, Regulation Z credit cards, and products or services that facilitate payments from a Regulation E account or a Regulation Z credit card."[50] Put more simply, the NPRM proposes to cover only depository institutions, card issuers, and "other payment facilitation providers." This scope is far too narrow in light of the financial lives of many consumers. Consumers utilize a wide swath of financial products and services, much broader than just consumer asset accounts and credit card accounts. Moreover, banks and nonbanks are competitively offering a variety of consumer financial products and services beyond those contemplated by the NPRM, leaving a gap in consumer protection based on what specific products or services a consumer is utilizing. As CBA outlined in response to the CFPB's Small Business Regulatory Enforcement Fairness Act (SBREFA) outline[51] concerning consumers' personal financial data rights and the pending rulemaking pursuant to Section 1033 of the Dodd-Frank Act:

> *To promote competition and genuinely benefit consumers, the Bureau should adopt a broader scope of coverage for data providers and regulate the following accounts and products under a Section 1033 rule: Regulation E accounts; Regulation Z credit card accounts; brokerage accounts;[52] nonbank mortgage accounts; captive auto loan accounts; digital wallets not otherwise an account under Regulation E; cryptocurrency accounts; alternative loans, such as buy-now-pay-later (BNPL) products; and any other product or service defined as a "consumer financial product or service" under the Dodd-Frank Act. Any entity – bank or nonbank – offering the above listed accounts or products is offering a consumer financial product or service, and thus should comply with any obligations imposed on data providers. This will result in data provider obligations applying not only to insured depository institutions and card issuers, but also to nonbanks providing accounts and products that likewise implicate payments and transaction data.*[53]

---

[50] 88 Fed. Reg. at 74803.

[51] 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), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

[52] Any supervision by the Bureau in connection with brokerage accounts under the scope of a Section 1033 final rule should be performed on data providers already subject to supervision by the Bureau. To the extent that an entity offering brokerage accounts is registered with the Securities and Exchange Commission (SEC), such entity should not be subject to the Bureau's supervisory authority following the finalization of this rulemaking. However, the foregoing does not limit the ability of the SEC itself to supervise any such SEC-registered entity.

[53] CBA, *Feedback on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives under Consideration* (Jan. 25, 2023), https://www.consumerbankers.com/sites/default/files/CBA%20Comment%20on%20CFPB%20SBREFA%20Outline%20for%20Rulemaking%20on%20Personal%20Financial%20Data%20Rights.pdf

The NPRM states the Bureau intends to implement Section 1033 with respect to other covered persons and consumer financial products or services through supplemental rulemaking,[54] though no time frame has been provided for such supplemental rulemaking and there will be little time after the finalization of the current rule for the Bureau to initiate a follow-up rulemaking before the next Presidential election which could result in a change in leadership at the Bureau. Even if the Bureau insists on a staggered approach to coverage of consumer financial products and services under a Section 1033 final rule, the Bureau could instead adopt a staggered compliance timeframe for products, rather than relying on a supplemental rulemaking that may not actually happen. Providing certainty to the market will also drive efficiency, spur innovation, and may reduce the time needed to come into compliance as systems can be designed holistically rather than by patches and workarounds, which could have lasting impacts on the ability for market wide standards being adopted. Indeed, as discussed in Part IX, the Bureau has already shown a willingness to pursue staggered timelines with respect to obligations under Section 1033.

Expanding the scope of coverage through an additional proposed rule before finalization of this rulemaking would also be consistent with Director Chopra's assertion that information captured from accounts is meant to assist industry in underwriting or helping consumers access new products,[55] such as allowing consumers to access covered data regarding all their accounts,[56] rather than just Regulation E asset accounts or Regulation Z credit card accounts,[57] would provide a more holistic picture of a consumer's financial health. CBA has previously advised the Bureau that "this adjustment would reflect the reality of the market today. Millions of consumers

---

[54] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74804 (Oct. 31, 2023).
[55] Consumers First: Semi-Annual Report of the Consumer Financial Protection Bureau Before the H. Comm. On Fin. Serv., 117th Cong. (2022) (response by Rohit Chopra, Director of the Consumer Financial Protection Bureau, to question by Rep. Hill (R-AR)), https://www.youtube.com/watch?v=I4A09yhfmyw.
[56] CBA also encourages the Bureau to further clarify the treatment of trust accounts. While the Bureau proposes to define the term "consumer" to include trusts established for tax or estate planning purposes, additional clarity is needed to ensure trust accounts are treated appropriately. Specifically, the Bureau should make clear whether the final rule applies to fiduciary accounts where a national bank acts as trustee and/or executor of a trust or estate that distributes fiduciary funds, electronically or otherwise, to an individual. The definition of consumer in the proposed rule defines consumer to be natural person, including a trust established for tax or estate planning purposes, but a trust is neither a natural person nor a legal representative of a person; it is a separate legal entity with a separate tax identification number. Further, the proposed rule defines a "covered consumer financial product or service" as an account defined in Regulation E, but accounts held pursuant to a bona fide trust agreement are carved out of the definition of account for Regulation E. *See* 12 C.F.R. 1005.2(b)(2); 12 C.F.R. Part 1005, Supp. I, cmt. 2(b)(2)-1. The two definitions plainly contradict one another. In addition, the Bureau should rectify any potential conflicts with a bank fiduciary's duty to keep bank records confidential, given that fiduciary accounts involving trust and estates often involving multiple beneficial interests.
[57] Under proposed section 1033.111(b) the definition of "covered consumer financial product or service" does not specify the rule applies only to *currently open and active* Regulation E accounts or Regulation Z credit cards. The Bureau should either in the regulatory text or supplemental commentary confirm that the obligations under the Section 1033 final rule apply to current and active accounts of the consumer, and that the provisions of the Section 1033 final rule are not applicable with respect to closed and inactive consumer accounts.

currently share their financial data on investment and mortgage accounts with third parties, which provides them with a holistic view of their finances."[58] Similarly, failing to include EBT accounts in the Bureau's rulemaking risks creating a two-tiered financial service system, in which lower-income consumers who have less access to traditional banking services have less transparency and control over their financial lives.[59]

B. Fees

The Bureau should allow data providers to charge reasonable and proportional fees to authorized third parties, or data aggregators acting on behalf of third parties, accessing the developer interface.

Data providers should be permitted to charge reasonable and proportional fees to authorized third parties, or data aggregators acting on behalf of third parties, accessing the developer interface as a natural part of the data provider's business model, distributing market-based costs and risk allocation, and for offsetting the costs that data providers will face in subsidizing the creation of and performing operational maintenance activity for this entire data access ecosystem.

As an initial matter, under the NPRM as drafted, data aggregators would be permitted to charge fees to downstream parties receiving covered data, yet data providers are not permitted to charge fees for making the data accessible to data aggregators or downstream parties receiving covered data. To the extent that data aggregators are able to charge fees while data providers cannot, third parties that pay data aggregators are likely to pass on those fees to the consumer, creating an anticompetitive windfall for data aggregators at the expense of a competitive market and all other participants in the data access ecosystem. Such an imbalance is inconsistent with the Bureau's goal to promote a fair and equitable system. This imbalance would be partially offset if data providers are likewise allowed to charge reasonable and proportional fees for accessing the developer interface.

---

[58] CBA, *Feedback on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives under Consideration* (Jan. 25, 2023), https://www.consumerbankers.com/sites/default/files/CBA%20Comment%20on%20CFPB%20SBREFA%20Outline%20for%20Rulemaking%20on%20Personal%20Financial%20Data%20Rights.pdf

[59] *See, e.g.*, Beek Center for Social Impact and Innovation at Georgetown University et al., *Comment Letter to CFPB Director Rohit Chopra* (Jul. 27, 2023), https://www.clasp.org/wp-content/uploads/2023/07/CLASP-Sign-On-Letter-EBT-Accounts-Section-1033-Rule-July-2023.pdf ("This two-tier system results in fewer rights and consumer protections for Americans who have low incomes and who may have less access to traditional banking services when compared with consumers who have higher incomes. This is inequitable and will exacerbate hardship for people living in poverty."); Ariel Kennan, Beeck Center, "EBT Users Deserve Data Rights" (Jan. 20, 2023), https://beeckcenter.georgetown.edu/ebt-users-deserve-data-rights/ (last visited Dec. 17, 2023) ("Ultimately, EBT users deserve the same class of service and protection as users of other consumer financial products. They should have access to their data and the ability to utilize third-party services to view and analyze their data, whether for scanning for fraudulent transactions or managing their financial outlook.").

Additionally, the Bureau's justification for limiting fees charged by data providers similarly supports limiting the ability of data aggregators to charge fees. The Bureau reasons that fee restrictions are permissible on data providers because "prolonged negotiations about fees could delay or obstruct third parties being granted access expeditiously to data providers' developer interfaces, in turn undermining the core consumer data access right."[60] This logic also applies to the fee negotiation between data aggregators and third parties; as a result, based on the Bureau's own logic in justifying fee restrictions on data providers, data aggregators should similarly not be permitted to charge fees. Moreover, Congress has historically been very clear when it wants fees to be treated in a certain manner and when it is empowering a regulator to set fees related to consumer finance. For example, the Fair and Accurate Credit Transactions Act[61] amended the FCRA to provide consumers with a right to receive one free credit report every year.[62] Similarly, the Credit Card Accountability Responsibility and Disclosure Act[63] amended the Truth in Lending Act[64] to, among other things, outline requirements related to late fees[65] and prohibit certain types of fees, such as double-cycle billing and penalties for on-time payments.[66] Section 1033 contains no analogous language relating to fees, suggesting that Congress did not view Section 1033 as empowering the Bureau to prohibit fees in connection with the consumer access to data.

The Bureau severely underestimates the costs that data providers will face in building out this data access ecosystem. Data providers will need to fund the creation of developer interfaces that meet the Section 1033 final rule's requirements, including functions or standards that have not actually been fully defined or clarified. Even where a data provider has established an API for authorized third party data sharing, the Bureau's current proposal would require issuers to make significant modifications, including the scope, format, and availability of the interface. At least one CBA member has roughly estimated these conversion costs to be in the high tens of millions of dollars. As discussed later in this letter,[67] some of these standards may not even be established at the time a data provider's systems are required to be compliant. As summarized in Part IX, the Bureau has significantly overestimated the ease with which the developer interfaces can be developed and implemented by data providers, and for institutions creating a new developer interface from the ground up the costs will be significant.

---

[60] 88 Fed. Reg. at 74814.
[61] Public Law 108-159, 117 Stat. 1952 (2003).
[62] 15 U.S.C. § 1681j(a).
[63] Public Law 111-24, 123 Stat. 1734 (2009).
[64] Public Law 90-321, 82 Stat. 146 (1968).
[65] *See* 15 U.S.C. § 1637(b)(12).
[66] *See* 15 U.S.C. § 1637(j).
[67] *See infra* Part IX.

Data providers also face significant costs with the maintenance of developer interfaces. Some data providers currently spend millions of dollars each year maintaining their pre-existing systems and would need to spend millions more to create the new infrastructure for the Section 1033 final rule. Further, in the NPRM as drafted, data providers would play an outsized role in monitoring the compliance of third parties and data aggregators with their own obligations,[68] a policing function that would entail additional costs, responsibilities, staffing, and risks. Based on the specific use cases and information an authorized third party or their data aggregator is accessing, data providers may have heightened risk management, fraud prevention, or other obligations that incur their own unique set of costs. Even the altered scope of covered data that data providers must make available does not mitigate these concerns. For example, one set of "covered data" is transaction information, including historical transaction information, and requiring institutions to make available through a developer interface more historical transaction information than they otherwise make available, will necessarily entail additional costs.

These numerous additional costs could be offset by imposing fees on other parties in the data access ecosystem. The costs to data providers could be paid for by consumers directly, such as through higher account maintenance fees, or indirectly, such as through a reduction in services offered by data providers. However, passing costs on to consumers or reducing services would be a perverse outcome that undercuts the purpose of the Section 1033 rulemaking in the first place. It follows then that additional costs must be borne by third parties and data aggregators accessing the consumer's data. Importantly, this approach can allocate costs in a targeted manner. If the costs are borne by consumers, it would affect *all consumers*, as all would be affected by actions like a data provider reducing the number of services they offer. If the costs are borne by authorized third parties and data aggregators though in the form of a fee, only authorized third parties and data aggregators actually accessing covered data through a developer interface would incur a fee from any particular data provider at a particular time. Such a fee can be tied to the number of access attempts, or amount of covered data accessed, by a third party or data aggregator. In this case, third parties that do not benefit from the use of data sharing would not be obligated to contribute to the costs associated with offering data. Authorized third parties and data aggregators accessing more data through developer interfaces would necessarily incur greater fees than those accessing less data, a principle which is equitable for all participants in the data access ecosystem and prevents any one party from shouldering the financial burden. This also would incentivize the goals of data minimization as authorized third parties will truly only seek data needed to provide the given product or service.

[68] *See infra* Part IV.

C. Frequency of Access

The Bureau should clarify what makes an access cap "unreasonable" and declare it is reasonable for a data provider to limit an authorized third party's or data aggregator's access if there is a risk the authorized third party's or data aggregator's repeated access attempts may cause unreasonable technical strain on the data provider's system or hinder the ability of other authorized third parties and data aggregators to access the developer interface.

Not only does the NPRM obligate data providers to provide covered data through developer interfaces they have funded, but data providers under the NPRM lack the ability to meaningfully control or limit the amount of times the developer interface is accessed by an authorized third party or a data aggregator. The proposed regulatory text states that "a data provider must not unreasonably restrict the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface. Any frequency restrictions must be applied in a manner that is nondiscriminatory and consistent with the reasonable written policies and procedures that the data provider establishes and maintains… Indicia that any frequency restrictions applied are reasonable include that they adhere to a qualified industry standard."[69] The NPRM asserts this provision is necessary because "access caps can prevent consumers from obtaining their most up-to-date data when a third party has surpassed its data limit. The removal of unreasonable access caps under the proposed rule would reduce such issues."[70]

The Bureau fails to define what an "unreasonable" restriction on the frequency of access by an authorized third party or data aggregator would be, and simply states it is an "indicia of compliance" if the data provider is complying with a recognized industry standard, which may not even exist at the time some entities are required to be in compliance with the rule.[71] This access cap provision also fails to acknowledge the market reality that very large data aggregators may crowd out other authorized third parties and smaller data aggregators attempting to access the developer interface. If the largest data aggregators can freely and continually access a data provider's developer interface to the point where it causes technical strain on the developer interface's functionality, this would hinder the ability of all other authorized third parties and data aggregators to access that same developer interface. To that end, the Bureau should clarify what makes an access cap "unreasonable," provide examples, and recognize that it is reasonable for a data provider to limit an authorized third party's or data aggregator's access if there is a risk that such authorized third party's or data aggregator's repeated access attempts may cause unreasonable technical strain on the

[69] 88 Fed. Reg. at 74871.
[70] 88 Fed. Reg. at 74856.
[71] *See infra* Part IX.

data provider's system or otherwise hinder the ability of other authorized third parties and data aggregators to access the developer interface.

D. Authorization and Authentication

The Bureau should:

- ***Affirm data providers have the right, but not obligation, to confirm a third party has followed the authorization procedures.***
- ***Permit, but not require, data providers to confirm additional aspects of the scope of authorization as may be reasonably necessary and appropriate.***
- ***Clarify that a revocation method being "reasonable" does not limit a data provider's ability to provide clear disclosures about data access to their consumers.***
- ***Allow consumers to modify the scope of an authorized third party's authorization without needing to terminate the authorization entirely.***
- ***Review authorizations as part of the Bureau's supervision of third parties and data aggregators.***

CBA is supportive of the NPRM's requirement that data providers must authenticate the identity of both the consumer and the authorized third party.[72] CBA also supports the option given to data providers to confirm the scope of the authorized third party's authorization directly with the consumer.[73] Data providers being able to authenticate and confirm authorization is vital for the protection of consumers from fraud and manipulation. Unfortunately, some of the proposals for confirming authorization would be impractical to implement as currently drafted. Proposed section 1033.331(b)(2) states "[t]he data provider is permitted to confirm the scope of a third party's authorization to access the consumer's data by asking the consumer to confirm: (i) [t]he account(s) to which the third party is seeking access; and (ii) [t]he categories of covered data the third party is requesting to access, as disclosed by the third party pursuant to § 1033.411(b)(4)."[74] Data providers should be *permitted, but not required*, to confirm additional aspects of the scope of authorization as may be reasonably necessary and appropriate, including for purposes of complying with safety and soundness or risk policies and procedures. As the data access ecosystem continues to develop and evolve, there may be other integral aspects to authorization that data providers would be best positioned to confirm to protect consumers. For example, if consumers are able to eventually grant a third party permission to access covered data for different durations in connection with different use cases, it would be important for data providers to confirm the scope of the duration of access that the consumer authorized for the third party for a specific use case. To avoid increasing the risk of consumer harm as the data

[72] 88 Fed. Reg. at 74,871.
[73] 88 Fed. Reg. at 74871.
[74] *Id*. at 74871-72.

access ecosystem advances, the Section 1033 final rule should provide leeway for data providers to confirm different aspects of the scope of authorization that may not be contemplated as of today. Moreover, authorizations should be reviewed by the Bureau as part of their supervision of third parties and data aggregators in the data access ecosystem.

Data providers under proposed section 1033.331(e) are permitted to make available to a consumer a method to revoke a third party's authorization, but such method of revocation "must, at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party."[75] While CBA approves of the ability of data providers to share a revocation method with consumers, CBA recommends that the Bureau clarifies that the requirement such revocation method be "reasonable" does not limit a data provider's right to provide their consumers with clear disclosures about who may access the consumer's data and how such data may be used, nor should data providers be limited in sending periodic reminders to consumers that their data is being accessed by third parties. These disclosures are vital for the protection of consumers by their data providers.

Additionally, consumers should be permitted to modify the scope of an authorized third party's authorization without needing to terminate the authorization entirely. Consumers may consent in their initial authorization to share covered data from multiple accounts with an authorized third party, yet at a later data wish to revoke the authorized third party's access to only one of the accounts. The NPRM though explicitly states:

> *Proposed § 1033.331(e) would not permit a data provider to make available a method through which the consumer could partially revoke a third party's access to the consumer's data, i.e., revoke access to some of the data the consumer had authorized the third party to access, but not other data it had authorized under the terms of the same authorization. For example, if the consumer consented in the initial authorization to share their deposit account and credit card data with a third party, the data provider could not make available a revocation method through which the consumer could revoke access to the deposit account but not the credit card account. Such a revocation method would be inconsistent with proposed § 1033.201(a), which would require data providers to make covered data available upon request based on the terms of the consumer's authorization. In addition, consumers who partially revoke access to their data could unintentionally disrupt the utility of data access for certain use cases.*[76]

[75] *Id.* at 74872.
[76] *Id.* at 74825.

This limitation is directly counter to the principle that the consumer is ultimately in control of their data,[77] which is a fundamental underpinning of not just Section 1033, but open banking more generally. The NPRM warns that consumers partially revoking access could disrupt certain use cases, yet this concern about disruption should not override the consumer's control of their own data. There could be reasons for any particular consumer that they may initially consent to sharing deposit account and credit card covered data, then at a future time may wish to no longer share data from one of those accounts (i.e., a consumer may initially consent to sharing deposit account and credit card covered data, then later change their mind with respect to only the credit card covered data).

Finally, proposed section 1033.331(b)(1)(iii) obligates data providers to make covered data available after receiving information sufficient to confirm the third party has followed the authorization procedures.[78] The proposed text does not appear to obligate data providers to actually confirm the authorization procedures before making the covered data available. CBA requests that the Bureau confirms this understanding of a data providers' obligations under proposed section 1033.331(b)(1)(iii) is correct. It would be a significant obligation if the Bureau were to require data providers monitor the behavior of all third parties accessing their developer interfaces instead of affording data providers a right to confirm the third party has followed the necessary authorization procedures. It is not feasible for a single data provider to manually review the terms and conditions of thousands of authorized third parties accessing the developer interface to ensure compliance with all authorization procedure obligations. It may also not be feasible for a data provider to determine what was or was not provided by the authorized third party to a specific consumer. It is important that the Bureau affirms that data providers have the right, rather than the obligation, to confirm the third party has followed the authorization procedures and are afforded a reasonable time to do so prior to requiring data be made available. This would still allow data providers to protect consumers and perform necessary due diligence on certain third parties, without requiring data providers to spend innumerable resources on reviewing the authorization procedures process of all third parties.

---

[77] Under proposed section 1033.331(d), for a jointly held account a data provider must make covered data available if the request comes from the consumer or an authorized third party acting on behalf of the consumer. Consistent with the principle that Section 1033 is fundamentally centered on a consumer's *access* to information, the Bureau should clarify that "authorized users" of an account should not have permission to access covered data for that account because they are not the holder of the account. For example, if a consumer adds a relative as an authorized user to their credit card account, the relative should not be able to allow permission to a third party to access covered data from the data provider related to that consumer's credit card account.

[78] 88 Fed. Reg. at 74871.

E. Conditions of Access

The Bureau should specify that denying a third party access to a developer interface based on guidance issued by prudential regulators with respect to third party risk management is a reasonable denial.

The Bureau should further consult with the prudential regulators to ensure that data providers have appropriate third party risk management obligations for managing access to covered data by third parties through a developer interface. The Bureau should also continue to regularly consult the prudential regulators on an ongoing basis as the data access market continues to develop and evolve. Proposed section 1033.321(a) permits data providers to reasonably deny a third party access to the developer interface based on risk management concerns.[79] The NPRM as drafted indicates indicia that whether a denial is reasonable includes if the denial was related to data security or risk management.[80] While CBA appreciates that the Bureau seeks to prevent potential anticompetitive behavior by data providers that may improperly deny access to third party competitors, many data providers will have obligations from the prudential regulators to manage risk to protect the safety and soundness of the financial system. These prudential risk management obligations will necessarily factor heavily into data providers' determination whether to deny a third party's or data aggregator's attempt to access a developer interface and may be significantly impacted by the amount of data requested by the authorized third party.

The Bureau should revise proposed section 1033.321(a) to specify that a bank denying a third party access to a developer interface based on guidance issued by prudential regulators with respect to third party risk management is a reasonable denial.[81] This approach would ensure that all data providers are able to protect the safety and soundness of the financial system as a whole. While the Section 1033 final rule will facilitate greater access by third parties to covered data held by data providers, access cannot come at the expense of a stable and secure financial ecosystem.

III. Covered Data

The NPRM outlines six categories of "covered data" that a data provider would be required to make available through a developer interface: (i) transaction information, including historical transaction information in the control or possession of the data provider; (ii) account balance; (iii) information to initiate payment to or from a Regulation E account; (iv) terms and conditions; (v) upcoming bill information; and (vi)

---

[79] *Id.*
[80] *Id.*
[81] If a data provider is not subject to prudential regulation on third party risk management, the Bureau should consult with the prudential regulators and consider subsequently issuing guidance for those data providers that is equivalent to, but no more burdensome than, the third party risk management guidance from prudential regulators that would provide similar cause of reasonable denials.

basic account verification information. CBA discusses concerns related to each of the categories of "covered data" in turn below.

A. Transaction Information

The Bureau should:

- ***Require data providers to share only transaction information they already retain and explicitly acknowledge that data providers are not required to retain any new records about a consumer.***
- ***Obligate data providers to make 12 months, rather than 24 months, of historical transaction information available.***
- ***Do not mandate data providers share reward credits per transaction.***

The first category of "covered data" that data providers would be required to make available would be transaction information, "including historical transaction information in the control or possession of the data provider."[82] The obligation for data providers to maintain historical transaction information appears to be inconsistent with Section 1033(c), which provides that "[n]othing in [Section 1033] shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer."[83] The Bureau in the NPRM reasons that Section 1033(c) "merely provides that a covered person is not required to maintain or keep additional information on a consumer and is silent as to record retention relating to compliance with [Section 1033] itself."[84] This category of transaction information could include amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges.[85]

To the extent that data providers are sharing this information, it is imperative that the final rule acknowledge that data providers are only obligated to share information that they already retain, and data providers are not required to retain any new records about a consumer in order to comply with the rule's obligation to make transaction information available. A failure to explicitly include this language could lead to the requirement of sharing certain transaction information in the future potentially running afoul of Section 1033(c). Additionally, the Bureau should reconsider the inclusion of a transactions "pending or authorized status," as pending transactions may change before being settled. Errors within the financial marketplace, including an inaccurate picture of a consumer's financial health, are likely to increase when a third party can receive information about a pending transaction, but that transaction's information later changes.

---

[82] 88 Fed. Reg. at 74870.
[83] 12 U.S.C. § 5533(c).
[84] 88 Fed. Reg. at 74829.
[85] *Id.* at 74870.

The NPRM also indicates that a data provider would be deemed to "make available sufficient historical transaction information… if it makes available at least 24 months of such information."[86] The Bureau supports this time frame by arguing "24 months would be consistent with the recordkeeping requirements in Regulation E and Regulation Z"[87] and "data providers typically control or possess more than 24 months of historical transaction data and continue to make more than 24 months available."[88] As a preliminary matter, the Bureau should not impose any net new retention requirements on data providers greater than those contained under the appropriate regulatory regime for each product for which covered data must be made available pursuant to the Section 1033 final rule. Consistent with this guiding principle, the Bureau should impose a flat availability timeframe for all data providers. The Bureau bases the historical transaction information availability requirement on Regulation E and Regulation Z, yet if the Bureau adopts CBA's recommendations in Part II.A of this letter to expand the scope of covered data providers, there may be several covered products or services subject to regulatory regimes with retention requirements shorter than the 24-month requirements under Regulation E and Regulation Z. It is important that all entities operating as data providers under the Section 1033 final rule be subject to the same type of retention requirements. Moreover, there is a difference for data providers in the systems and costs needed for retaining information consistent with regulatory expectations and making that same period of information available to third parties and data aggregators through a developer interface. In recognition of the variety of potential retention requirements for products in an expanded scope of coverage, the Bureau should require that data providers only make 12 months, rather than 24 months, of historical transaction available.

It is also unreasonable for data providers to be obligated to share reward credits per transaction.[89] As an initial matter, obligating data providers to share reward credits per transaction will necessitate the development of costly new technologies to share this information, which is a significant cost unaccounted for in the NPRM without a tangible consumer benefit. Even though some consumers may be able to interact with a customer service professional at their card issuer to obtain information about credits per transaction, the NPRM proposes sharing this information through an entirely new costly channel. The sharing of this information will be further complicated by the fact that different rewards credits may be valued differently, which is a nuance that may not be understood by a third party or data aggregator performing a data pull for this information. It is currently more common in the market to share total reward balance, rather than reward credits per transaction. Shifting from this model to sharing a different set of information regarding rewards would place a significant burden on data

[86] *Id.*
[87] *Id.* at 74811.
[88] *Id.*
[89] The NPRM uses the term "rewards credits." CBA understands the Bureau to be referring to "reward credits per transaction." The Bureau should immediately clarify to industry if the Bureau is using the term "rewards credits" to refer to something else.

providers and increase costs that all data providers will face. For many data providers, information regarding reward credits per transaction are the result of that data provider's proprietary algorithm that classifies merchants into different reward point categories. Failing to classify this information as confidential commercial information is misguided and will harm consumers in the long term. If information regarding reward credits per transaction are made available to third parties, third parties may be able to use this information to reverse engineer the proprietary algorithms that data providers have invested significant time, effort, and funds into. As a result, data providers would be disincentivized from creating increasingly sophisticated algorithms to enhance consumers' rewards experiences, as information produced by these algorithms would be immediately accessible to competitors that could then reverse engineer the algorithms without the same level of effort and resources dedicated to its production. The net result will be that data providers stop investing in increasingly enhanced algorithms related to reward credits, which will harm consumers in the aggregate, particularly those who most value their rewards programs. The Bureau should also clarify that, to the extent that rewards-related information is required to be shared under the Section 1033 final rule, data providers should not be required to share any rewards-related data that they themselves do not own, generate, or possess. This clarification is necessary in light of the fact that some data providers' partners may consider their rewards-related information to be proprietary information that the data provider is prohibited from externally sharing. The Bureau should also clarify that rewards-related information not connected to a financial product or service would not be covered under a Section 1033 final rule. Requiring data providers to share such information would not further the Bureau's goal of allowing consumers to compare different financial products or services because these types of rewards could be earned with or without the consumers' particular product or service.

B. Account Balance

The Bureau should provide additional examples of "account balance" to assist data providers in complying with the final rule.

The second category of "covered data" would be account balance, which would include available funds in an asset account and any credit card balance.[90] The Bureau has asked for information as to whether the term "account balance" is sufficiently defined or whether additional examples of account balance, such as the remaining credit available on a credit card, are necessary.[91] CBA is supportive of the Bureau providing the greatest degree of clarity and meaningful guidance to industry to facilitate compliance with the Bureau's rulemakings. As such, any additional examples of "account balance" that the Bureau outlines in the final rule will be a helpful tool for industry compliance.

[90] 88 Fed. Reg. at 74811.
[91] *Id.*

C. Information to Initiate Payment to or from a Regulation E Account

The Bureau should:

- ***Not mandate sharing information to initiate payment to or from a Regulation E account.***
- ***To the extent information to initiate payment to or from a Regulation E account is required to be shared by data providers, place appropriate liability obligations on third parties in recognition of the increased liability risk that data providers will face.***

The Bureau proposes that the third category of "covered data" be information sufficient to initiate payment to or from a Regulation E account and would include a tokenized account and routing number that can be used to initiate an Automated Clearing House (ACH) transaction.[92]

As a threshold matter, the language of Section 1033 is centered on a consumer's *access* to information, yet this type of information is being shared in order to, according to Director Chopra, "underwrite or help people access new products…. "[93] This is a significant extension beyond the statute's plain language. Particularly in light of Director Chopra asserting that "[a] key priority for the CFPB is to help accelerate the shift to open banking and payments," all stakeholders must carefully make sure that the Bureau's reach does not exceed the authority granted to it by Congress.[94] Director Chopra has made sweeping, grandiose speeches about ushering in "a new competitive market," but it isn't clear if the limited language of Section 1033 is sufficient or robust enough to constitute Congressional authority for the Bureau to impose changes of such economic and political significance.[95] Moreover, it is unclear how sharing this information would actually benefit consumers, as this information does not seem pertinent to enabling industry to "underwrite or help people access new products"[96] in the same way that other contemplated "covered data" could facilitate these purposes. In the absence of a robust explanation for how this data can meaningfully assist with consumer access to products, data providers should not be required to share it,

---

[92] *Id.* at 74870.

[93] Consumers First: Semi-Annual Report of the Consumer Financial Protection Bureau Before the H. Comm. On Fin. Serv., 117th Cong. (2022) (response by Rohit Chopra, Director of the Consumer Financial Protection Bureau, to question by Rep. Hill (R-AR)), https://www.youtube.com/watch?v=I4A09yhfmyw.

[94] Rohit Chopra, Dir., Consumer Fin. Prot. Bureau, *Prepared Remarks of CFPB Director Rohit Chopra at the Federal Reserve Bank of Philadelphia's Annual Fintech Conference* (Sept. 7, 2023), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-federal-reserve-bank-of-philadelphias-annual-fintech-conference/.

[95] Rohit Chopra, Dir., Consumer Fin. Prot. Bureau, *Prepared Remarks at Money 20/20* (Oct. 25, 2022), https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/.

[96] Consumers First: Semi-Annual Report of the Consumer Financial Protection Bureau Before the H. Comm. On Fin. Serv., 117th Cong. (2022) (response by Rohit Chopra, Director of the Consumer Financial Protection Bureau, to question by Rep. Hill (R-AR)), https://www.youtube.com/watch?v=I4A09yhfmyw.

especially given the significant risks posed to providing the information that could be used to initiate unauthorized transfers and the potential costs to data providers. As proposed, even the most compliant data provider is at a significant risk of loss due to no fault of their own when sharing this data element with an authorized third party.

Nonetheless, it is heartening that the Bureau in the NPRM acknowledges that industry can share tokenized account numbers (TANs) with third parties in lieu of full account and routing numbers. CBA in its comment on the SBREFA outline warned about the dangers of sharing non-tokenized account and routing numbers:

> *The financial services industry has steadily been moving toward tokenization of deposit account and routing numbers to provide greater consumer protection and control, as well as to decrease fraud. It is vital that data providers have the option to share a tokenized deposit account and routing number - rather than the actual account number and routing number - with authorized third parties. If data providers are not allowed to share the tokenized deposit account and routing number in lieu of the actual deposit account and routing number with third parties, additional and unnecessary risk would be introduced into the payments ecosystem, increasing consumer harm. For example, third parties, or any other entities that gain access to this information, could initiate fraudulent transactions or engage in other criminal activity utilizing a consumer's actual deposit account number and routing number.*[97]

The sharing of information for initiating a payment to or from a Regulation E account, particularly the sharing of non-tokenized account and routing numbers, will make third parties an increased target for data breaches. Compromised credentials could be used to initiate fraudulent transactions, which would not only harm consumers, but also drastically expand the liability that will rest with either data providers or with consumers. Beyond the concerns outlined later in this letter regarding liability,[98] the liability risk related to this specific covered data is magnified because of the differences for liability allocation under the NACHA Rules compared to Regulation E.

The NACHA Rules apply to consumer ACH credit and debit payments, most of which are also subject to Regulation E. Both the NACHA Rules and Regulation E provide a framework for treatment of unauthorized consumer ACH transactions, though they may apply in different ways and offer different liability concerns for data providers and consumers. The NACHA Rules allow consumers 60 days to instruct their bank (the

---

[97] CBA, *Feedback on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives under Consideration* (Jan. 25, 2023), https://www.consumerbankers.com/sites/default/files/CBA%20Comment%20on%20CFPB%20SBREFA%20Outline%20for%20Rulemaking%20on%20Personal%20Financial%20Data%20Rights.pdf.

[98] *See infra* Part VIII.

RDFI) that a specific ACH debit from their account is invalid.[99] If the consumer submits a written statement supporting that the debit was not authorized within the 60-day timeframe, the RDFI will return the transaction to the originating institution (the ODFI).[100] The ODFI, which originated the debit, has five days to dishonor the return. Reasons for a dishonored return include that the return is untimely, contains incorrect information, or was misrouted.[101] This 60-day rule differs from Regulation E's 60-day rule, under which a consumer must generally report unauthorized transfers within 60 days of their appearance on a periodic statement and then the consumer's bank must investigate that assertion.[102] If a consumer fails to notify their bank within the 60-day window, the consumer is liable for all unauthorized transactions that occur *after* the 60-day period.[103] NACHA, on the other hand, has a separate 60-day period for each transfer.

So, if a consumer has monthly unauthorized transactions but does not assert a claim until many months have passed, under Regulation E the consumer can only be reimbursed for the transactions that occurred up to, and until, 60 days after receipt of the periodic statement listing the first unauthorized transaction; the consumer will not be reimbursed for the unauthorized transactions that occurred after that date. However, under the NACHA Rules, the consumer can count back 60 days from the date when the consumer first asserts an error. In other words, under Regulation E, a consumer can always assert a transaction is unauthorized if that transaction occurred *before* the end of the 60-day period, whereas NACHA allows consumers to always count back 60 days from the day they *discover* unauthorized transactions.[104] As a result, data providers face increased liability risk in connection with ACH transactions because of the extended timeframe for which consumers can assert that a transaction is unauthorized and, if a data provider is an ODFI, that data provider also would be obligated to immediately return the funds to the RDFI unless it has dishonored the return.

Based on the foregoing, CBA recommends that the Bureau reconsider whether data providers should be obligated to share information to initiate payment to or from a Regulation E account. If the Bureau insists on requiring data providers share this information, then in recognition of the enhanced liability risk that data providers will

---

[99] *See* NACHA Operating Rules App'x 4, Table 4.2 (explaining that for return code R11, "Customer Advises Entry Not in Accordance with the Terms of the Authorization," the consumer's bank has 60 days to return the transaction); *see also* NACHA Guidelines Ch. 45 ("ODFIs, on behalf of their Originators, may receive PPD return entries as late as the opening of business on the banking day following the 60th calendar day following the Settlement Date.").
[100] NACHA Rule 3.12; *see also* 3.12.4 (detailing the contents of such a notice).
[101] NACHA Rule 2.13.6.1.
[102] 12 C.F.R. § 1005.6(b)(3).
[103] 12 C.F.R. Part 1005, Supp. I, cmt. 6(b)(3)-1.
[104] *See* NACHA, *Which 60 Days is It? Understanding the Different Periods in Regulation E and the Nacha Rules* (Aug. 17, 2021), https://www.nacha.org/news/which-60-days-it-understanding-different-periods-regulation-e-and-nacha-rules.

face, the Bureau should place further emphasis on third parties accepting liability obligations and ensuring they are adequately capitalized and maintain sufficient insurance. Whether such liability obligations are adjusted based on if TANs are used can be addressed through a variety of ways.

D. Terms and Conditions

The Bureau should:

- ***Only require a disclosure of a narrow set of discrete data elements – such as standard APR or APY – as part of making "terms and conditions" available.***
- ***Require sharing of realized fees, rather than the applicable fee schedule.***
- ***Do not require sharing of rewards program terms, whether a consumer has opted into overdraft coverage, and whether the consumer has entered into an arbitration agreement.***

The fourth category of "covered data" would be terms and conditions, which would include the applicable fee schedule, any APR or APY, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.[105] As a guiding principle the Bureau should only require a disclosure of a narrow set of discrete data elements – such as standard APR or APY – as part of making "terms and conditions" available under a Section 1033 final rule. This type of information is most readily comparable across accounts and would meaningfully facilitate underwriting and the offering of new consumer financial products or services by third parties accessing this information. To that end, rather than making the applicable fee schedule available, the Bureau instead should require that realized fees be shared. This information will provide a better understanding of true account costs for the specific consumer and facilitate the account-to-account comparisons the Bureau seeks to advance through this rulemaking and is usually included as part of the account statement.

The other items proposed to be shared as "terms and conditions" – rewards program terms, whether a consumer has opted into overdraft coverage, and whether the consumer has entered into an arbitration agreement – are not operationally practical to share and can change on a daily basis based on the consumer's own actions. Not all of these items are shared in pre-existing, quantifiable data fields given the significant variations and discrete elements they may have across data providers and consumers. These items are not readily reducible to a single discrete data element, and the NPRM as proposed would require data providers to turn over pages of account agreements for all their consumers to any third party that requests access. Sharing substantive, in-depth agreements goes far beyond a simple data pull by a third party, and nuances, such as

[105] 88 Fed. Reg. at 74870.

conditional terms that may or may not be applicable to a *specific* consumer's account, would not be captured in such a data pull by a third party. For example, reward program terms significantly vary across data providers, are product-specific, and some aspects are conditionally based on consumer behavior; there is no simple, discrete data element that can be pulled from these terms to assist in product comparison. These data pulls of significant, and sometimes lengthy, agreements by an ever-increasing number of third parties at an ever-increasing frequency will also place significant stress on the infrastructure underpinning these data providers' developer interfaces. Moreover, it is not clear what the actual benefit to the consumer would be in sharing this type of information, as information like standard APR or APY is more relevant for third parties underwriting or offering new consumer financial products or services to consumers than whether a consumer has elected to opt into overdraft coverage. In fact, this information may actually confuse or mislead consumers. To avoid consumer confusion, when regulators have wanted consumers to be able to compare different parts of terms and conditions, they have often required discrete elements be placed into a standard format; for example, credit card terms need to clearly be outlined in promotional material in a Schumer box or prepaid account short form disclosures.[106] Finally, there is an open question as to whether Section 1033 was meant to facilitate the sharing of these types of "terms and conditions." Section 1033 obligates covered persons to share "information relating to any transaction, series of transactions, or to the account *including costs, charges and usage data*."[107] The phrase "costs, charges and usage data" certainly would cover items like standard APR, APY, or realized fees. However, the other elements, such as whether a consumer entered into an arbitration agreement, do not seem to qualify as "costs, charges and usage data."

Finally, for several years the Bureau has regularly required that credit card issuers provide credit card agreements to the Bureau, which has then made those agreements available to consumers and any third party via the Bureau's credit card agreement database.[108] Earlier this year, the Bureau significantly expanded the scope of this information collection, in the name of increasing price competition in the credit card market and enabling comparison shopping.[109] Accordingly, it is unclear how the information the Bureau now seeks is not redundant with its other extensive regulatory reporting requirements, nor is it apparent that there is any incremental benefit to consumers that justifies the unnecessary potential cost and risk to consumers.

---

[106] *See* 12 C.F.R. § 1026.5; 12 C.F.R. § 1005.18(b)(2).
[107] 12 U.S.C. § 5533(a) (emphasis added).
[108] Consumer Financial Protection Bureau, Credit Card Agreement Database, https://www.consumerfinance.gov/credit-cards/agreements/ (last visited Dec. 17, 2023) ("The CFPB maintains a database of credit card agreements from hundreds of card issuers. Using the tool below, you can search for an agreement by the name of the issuer.")
[109] Consumer Financial Protection Bureau, *CFPB Enhances Tool to Promote Competition and Comparison Shopping in Credit Card Market*, March 21, 2023, https://www.consumerfinance.gov/about-us/newsroom/cfpb-enhances-tool-to-promote-competition-comparison-shopping-credit-card-market/.

E. Upcoming Bill Information

The Bureau should exclude third party bill payments that have been scheduled through the data provider from being shared.

The fifth category of "covered data" is upcoming bill information, which includes information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.[110] CBA recommends that the Bureau exclude information about third party bill payments that have been scheduled through the data provider. This is information that does not originate from a data provider, but instead is received from the consumer and not verified by a data provider prior to payment. Data providers are in the best position to share information generated by that data provider, as well as information about that data provider's customer; a data provider though is *not* in the best position to share information about a third party it does not have a primary relationship with, particularly when the source of that data providers' information is the consumer, rather than the third party itself. If the information is inaccurate and subsequently shared through a developer interface, errors will be introduced into the data access ecosystem that will be difficult to mitigate and could result in invalid or unauthorized transactions. Additionally, third party bill payment information raises concerns about the privacy of such third parties. As the NPRM is drafted, an authorized third party accessing upcoming bill information about a consumer will also be obtaining information about other third parties that consumer has paid, which could be other individuals. The pertinent information regarding recurring third party bill payments can already be identified by reviewing a consumer's transaction information, including historical transaction information, which would mitigate these privacy concerns.

F. Basic Account Verification Information

The Bureau should maintain the NPRM's narrow scope of basic account information category to name, address, email address, and phone number.

CBA supports the Bureau's decision to scale down the scope of the account verification information from the SBREFA outline. Under the SBREFA outline, there were fifteen pieces of "account identity information" under consideration, which included: (i) name; (ii) age; (iii) gender; (iv) marital status; (v) number of dependents; (vi) race; (vii) ethnicity; (viii) citizenship or immigration status; (ix) veteran status; (x) residential address; (xi) residential phone number; (xii) mobile phone number; (xiii) email address; (xiv) date of birth; (xv) Social Security number; and (xvi) driver's license number.[111] It

[110] 88 Fed. Reg. at 74,870.
[111] Consumer Financial Protection Bureau, *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives under*

was not clear what benefit these data elements would have provided to consumers in the data access ecosystem, and the potential misuses of this information by ill-intentioned third parties or fraudsters could have significantly harmed consumers. This is especially true as the consumer, rather than the data provider, is the true source of this information. None of the information is generated by the data provider or obtained through the ongoing use of the product or service. As such, CBA applauds the Bureau's decision to limit the basic account information category to name, address, email address, and phone number.[112] CBA notes, though, that even information like a consumer's address or email address is sensitive and could have implications beyond purely financial concerns. If the consumer wishes to provide information to the authorized third party, the consumer is in the best position to do that directly. For example, the leaking of a consumer's home address from a third party's data breach could implicate a consumer's personal safety. Due to the sensitivity of this information and the implications of its potential misuse, the Bureau should ensure that third parties and data aggregators have greater liability obligations in the Section 1033 final rule than they currently do under the NPRM.

IV. Screen Scraping

The Bureau should:

- ***Expressly prohibit the use of screen scraping by third parties and data aggregators of any data made available through a developer interface, not just covered data.***
- ***Shift the obligation away from banks and to the Bureau itself to supervise, assess, and pursue enforcement actions against third parties and data aggregators that improperly engage in screen scraping.***

The NPRM fails to actually prohibit the use of screen scraping by third parties and, as the NPRM is drafted, third parties could continue to use screen scraping to avoid the obligations the NPRM imposes on "authorized third parties."[113] CBA supports the Bureau's efforts to sunset the practice of screen scraping, but the NPRM does not effectively achieve that result. As CBA stated in response to the Bureau's SBREFA outline,[114] "[s]creen scraping is a fundamentally unsafe method of access, and the Bureau's Section 1033 rule should work to eliminate the practice by prohibiting third parties from attempting to screen scrape any information a data provider makes available via an API. Absent an express prohibition, it would be unduly costly for data

---

Consideration 22 (Oct. 27, 2022), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

[112] 88 Fed. Reg. at 74870.

[113] *See* 88 Fed. Reg. at 74873-75.

[114] 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), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

providers to effectively block screen scraping and push usage of safer APIs."[115] Importantly, screen scraping may cause consumer harm because, if a third party relies on screen scraping, "any tailoring of the consumer's authorization vanishes and a third party could have access to consumer information beyond what the consumer has authorized."[116] This information includes account information for products and services outside the scope of the NPRM. Moreover, if screen scraping is utilized during a service interruption, there is risk that a data provider would be unable to honor a consumer's authorization.

As a preliminary matter, the Bureau in the NPRM has essentially outsourced the monitoring and policing of third parties in the data ecosystem to data providers. This is misguided, and instead the Bureau should play a more significant role in taking action against third parties that screen scrape. The NPRM does not expressly mandate third parties use the developer interface, and necessarily become "authorized third parties," to access "covered data." As a result, even once a data provider has established a developer interface, third parties could still elect to engage in unsafe practices like screen scraping to access covered data and bypass the NPRM's obligations that protect consumers. Presumably data providers would still retain the ability to block third party access attempts outside of the developer interface with respect to covered data, but there is no actual obligation in the NPRM for data providers to do so. But given the Bureau's emphatic press statements and speeches about perceived competition concerns, every instance in which a data provider considers blocking screen scraping could turn into a lengthy and costly compliance and reputational risk exercise. Further, the proposal includes no language clarifying data providers' ability to block screen scraping as discussed below. Consistent with the following recommendations, the Bureau should expressly communicate to all market participants that engaging in screen scraping for data available through a developer interface is an inappropriate and dangerous practice and pursue enforcement actions against third parties that choose to screen scrape rather than utilize the developer interface.

The NPRM does not contain an express prohibition of screen scraping and, as drafted, appears to allow third parties to use screen scraping to bypass obligations they would otherwise have under a Section 1033 final rule. Under the NPRM, data providers are required to "make available to a consumer and *an authorized third party*, upon request, covered data in the data provider's control or possession."[117] To become an "authorized third party" that is able to access a data provider's developer interface, a third party

---

[115] CBA, *Feedback on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives under Consideration* (Jan. 25, 2023), https://www.consumerbankers.com/sites/default/files/CBA%20Comment%20on%20CFPB%20SBREFA%20Outline%20for%20Rulemaking%20on%20Personal%20Financial%20Data%20Rights.pdf.
[116] CBA, *Feedback on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives under Consideration* (Jan. 25, 2023), https://www.consumerbankers.com/sites/default/files/CBA%20Comment%20on%20CFPB%20SBREFA%20Outline%20for%20Rulemaking%20on%20Personal%20Financial%20Data%20Rights.pdf.
[117] 88 Fed. Reg. at 74870 (emphasis added).

must: (i) provide the consumer with an authorization disclosure, (ii) certify that the third party agrees to be bound by obligations related to the use, protection, and retention of consumers' covered data, among other obligations, and (iii) obtain the consumer's express informed consent to access covered data on the consumer's behalf.[118] In other words, the consumer protection obligations imposed by the NPRM on third parties are contingent on those third parties becoming "authorized third parties" in order to access the developer interface. If a third party is not seeking to access data through a developer interface, then there is no obligation in the NPRM for the third party to become an "authorized third party." Thus, consumer data accessed by these third parties will not be subject to the NPRM's obligations on third parties related to engagement with consumers, and data accessed outside of the developer interface will not have third party restrictions on use, resale, retention, etc., nor other applicable consumer protections under Section 1033.

The Bureau seems to have drafted the NPRM under the mistaken assumption that data providers are able to block all screen scraping attempts made through a consumer interface. No system maintained by a data provider can be entirely effective at blocking all screen scraping access attempts. Even for the largest data providers, it is complicated and expensive to differentiate and block automated web scraping while not inadvertently blocking real consumer traffic. Given the important focus on customer service, data providers generally err on permitting traffic rather than blocking real customer access. Distinguishing between the two has only become more difficult as third parties now regularly modify their automated scripts to appear more human and bypass efforts to restrict screen scraping. Efforts to counter screen scraping are akin to addressing each attempt individually as they occur. Even when efforts to block screen scraping are successful, consumers are still put at risk of harm because the third party or data aggregator will have collected the consumer's credentials to make the screen scraping attempt.

Additionally, as the NPRM is drafted, screen scraping would remain permissible for non-covered accounts; in other words, for any account that is not a Regulation E asset account or a Regulation Z credit card account, screen scraping would still appear to remain a viable option for third parties. This approach would result in the creation of a bifurcated data access ecosystem, in which developer interfaces would be used to access certain data that would be subject to various protections and use limitations, but screen scraping would be permissible for other data that would not have analogous protections and limitations. As a practical matter, the Bureau's proposal would continue to allow screen scraping of even covered account data because many data providers show consolidated account information via the consumer interface. Screen scrapers of non-covered accounts would thus also scrape covered account data and could apparently then sell such covered data or otherwise use it for the scraper's own profit under the NPRM. This would create a dangerous environment for consumer data.

[118] *Id.* at 74873.

It is also not clear under the NPRM whether data providers are obligated to permit screen scraping if developer interfaces do not meet certain minimum standards in specific instances. The NPRM provides that "[d]uring the rule's implementation period, and for data accessed outside its coverage, the CFPB plans to monitor the market to evaluate whether data providers are blocking screen scraping without a bona fide and particularized risk management concern or without making a more secure and structured method of data access available (e.g., through a developer interface)."[119] Elsewhere, the Bureau requires developer interfaces to meet minimum performance specifications, including that the number of proper responses by the interface divided by the total number of queries for covered data to the interface must be equal to or greater than 99.5 percent.[120] It is unclear whether a developer interface failing to meet minimum performance specifications within a given period would constitute a data provider not "making a more secure and structured method of data access available." In such instances, it is not readily apparent whether, in the absence of a particularized risk management concern, data providers would be required to permit screen scraping. Data providers should be expressly permitted to block screen scraping attempts if they make data available through a developer interface; the developer interface not meeting the exact minimum performance specifications at a specific point in time should not be treated as a developer interface not being made "available" for purposes of determining whether a data provider can block screen scraping.

The Bureau should have pursued other viable alternatives that would have more efficiently and meaningfully sunsetted the practice. At the very least, the Bureau could have obligated third parties to include in the certification statement a certification that they would not screen scrape any of the consumer's covered data. The Bureau could, alternatively, have also prohibited the screen scraping of any data – irrespective of whether that data is "covered data" under the final rule – that is made available through the developer interface. Indeed, the obligation of data providers to facilitate consumer access to information is "[s]ubject to rules prescribed by the Bureau."[121] The Bureau also has the authority under Section 1033 to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information,"[122] and limiting the ability of third parties to screen scrape directly is connected to the promotion of a standardized format for information through the developer interface. This approach would address several defects in the NPRM's approach. First, it would properly place the burden on third parties to not screen scrape, rather than requiring through regulation that data providers police third parties for compliance. Second, it would encourage data providers to share more data through the developer interface, which would facilitate consumer protection and accessibility to data. Third, making more data available through a developer interface should

[119] 88 Fed. Reg. at 74800.
[120] *See, e.g.*, id. at 74870-71.
[121] 12 U.S.C. § 5533(a).
[122] 12 U.S.C. § 5533(d).

encourage more third parties to access data through the developer interface rather than through screen scraping. This approach would be most effective if the Bureau – rather than data providers – supervised, assessed, and, if necessary, pursued enforcement against third parties[123] for compliance with their obligations under the Section 1033 final rule, including the obligation to not screen scrape consumer data made available through a developer interface.

V. Developer Interfaces

The Bureau should acknowledge an SSO, rather than the Bureau itself, is better positioned to advance reasonable standards for a developer interface.

As a general principle, any delegation by the Bureau to an SSO should be consistent with CBA's recommendation in Part VII of this letter that compliance with an SSO standard be treated as a sufficient, but not a necessary, condition for compliance with the Section 1033 final rule. This approach will ensure that evolving technologies and standards do not outpace compliance with the Section 1033 final rule. The Section 1033 rulemaking has taken over a decade to arrive at its currently proposed rulemaking stage, a result of the slow and deliberate process to create a durable final rule to underpin the data access ecosystem. Future rulemakings or attempts to amend the Section 1033 final rule in response to technological advances in the data ecosystem will likely not take another ten years, but will take significantly longer than it would for an SSO to change its standards or a data provider to address directly itself. This is particularly egregious when, as discussed in Part I.A, the industry is already independently making advancements toward creating the type of banking experience the Bureau seeks to foster.

If numerical standards are set by the Bureau through rulemaking, the Bureau will be locking industry into legacy technologies and standards that may not address needs in an evolving market. The setting of such numerical standards is not within the Bureau's remit under the statutory text of Section 1033, nor within the Bureau's expertise. Instead, SSOs or data providers would be able to move in a timelier, forward-looking market-driven manner to incorporate technological changes into their practices, benefitting consumers and authorized third parties.

Further, rather than issuing specific numerical standards, the lodestar for the Bureau and any SSO should be "reasonableness."[124] This assumes that data providers can

[123] To the extent that a nonbank third party would not be subject to supervision of the Bureau, the Bureau should utilize its risk-based supervision authority under 12 U.S.C. § 5514(a)(1)(C) and coordinate with other relevant state and federal entities, such as the Federal Trade Commission, to ensure supervision of these otherwise unsupervised nonbank third parties.

[124] An SSO being guided by a principle of reasonableness, rather than issuing specific numerical standards, should not preclude an SSO from publishing statistics or recommended practices with respect to items like response time or response rate.

alternatively demonstrate compliance with the rule by showing they acted "reasonably." Specifically, the Bureau should not mandate that a response time is not commercially reasonable if it is more than 3,500 milliseconds[125] nor that a response rate is commercially unreasonable if it is less than 99.5 percent.[126] A response time of 3,500 milliseconds fails to account for responses that contain larger payloads, such as lengthy transaction histories or customers with multiple accounts, peak seasonality, or potential external shocks. These responses may take more than 3,500 milliseconds while responses with less information will take less time. Additionally, response times may take longer due to data security concerns, such as the encryption process that a data provider may use for a response. This also appears to not take into account the time it may take to further analyze specific data requests to determine if a risk-based denial is warranted.

Similarly, mandating a response rate of at least 99.5 percent is ill-advised. Achieving a 99.5 percent response rate every month may be practically difficult, particularly when there may be channel outages. The Bureau mandates this 99.5 percent response rate while also providing little meaningful limitations on third parties access to data providers' servers, nor a meaningful avenue for data providers to recover reasonable costs. Even if such channel outages are addressed in a commercially reasonably rapid manner, a single brief outage could limit a data provider's ability to reach a 99.5 percent response rate in a given month. The implications of these aspects would be better understood and better evaluated by an SSO or data providers themselves in determining an ideal standard, rather than by the Bureau. For example, an SSO standard may evaluate that it is more practicable to evaluate the response rate on a three-month rolling basis, rather than a one-month basis, to prevent data providers being deemed noncompliant with the Section 1033 final rule because of a one-off outage, or other rare and unexpected events. SSOs can also assist data providers in acting reasonably by developing a utility that can intake and publish performance statistics to assist market participants in evaluating their systems' performances. It is also notable that the Bureau has imposed significant obligations with set numerical expectations on the market participants offering developer interfaces, but has not imposed numerical expectations on the parties accessing those developer interfaces.

Additionally, the Bureau should revise the retention periods for records related to developer interface responses to align with the record retention requirements contained elsewhere in the NPRM. Under proposed section 1033.351(d)(1), data providers must maintain "records related to a data provider's response to a consumer's or third party's request for information or a third party's request to access a developer interface… for at least three years after a data provider has responded to the request."[127] This three-year retention timeframe for response records is unique in the NPRM, particularly when

[125] 88 Fed. Reg. at 74871.
[126] *Id.*
[127] *Id.* at 74873.

retention timeframes elsewhere contemplated by the Bureau typically are 24 months.[128] The Bureau should align the developer interface response record retention requirements with general industry record retention requirements, but in no case should these retention requirements be greater than the general retention requirements of 24 months contained elsewhere in the NPRM.[129]

VI. Third Parties & Data Aggregators

CBA supports many aspects of Subpart D of the proposed regulatory text, which would impose a variety of obligations on third parties, and applauds the Bureau's efforts to provide transparency and clarity to consumers about how third parties and data aggregators access and subsequently use consumers' covered data. However, certain adjustments are needed to the authorization disclosure, certification statement, and description of third party obligations to ensure that consumers are well informed, and their data are adequately protected.[130]

A. *Authorization Disclosures*

The Bureau should require disclosure of complaint/dispute contact information for the third party and data aggregator (if applicable) as part of authorization disclosure.

The authorization disclosures that a third party must present to a consumer as described in proposed section 1033.411 should also include complaint and dispute information for all relevant parties. Consumers may mistakenly believe they should contact their data provider regarding any issues related to the sharing of covered data with third parties or data aggregators. However, if the Bureau adopts the recommendations in this letter, the more appropriate party for consumers to initially raise concerns with would be the third party or data aggregator. As such, any authorization disclosure provided by a data provider to a consumer should contain the complaint/dispute contact information for the third party, for the Bureau itself, and, if applicable, for the data aggregator. While proposed section 1033.421(g)(3) provides that contact information be provided to the consumer, it is important contact information sufficient to initiate a dispute and the Bureau's contact information are explicitly included in the initial disclosure provided to the consumer as consumers often refer to account, product, or service opening material when trying to determine who to contact. To assist third parties and data aggregators in complying with the

[128] *See* Part III.A (discussing whether data providers should be obligated to make 12 months or 14 months of historical transaction information available).
[129] The developer interface response record retention requirements, and the burden potential retention timeframes may impose on market participants, could be better evaluated if the Bureau were clearer on what information it contemplates being retained under this requirement.
[130] The Bureau should also clarify obligations in circumstances when a third party seeks authorization in connection with the use of one data aggregator, but then later switches to using a different data aggregator.

authorization disclosure requirement, the Bureau should provide safe harbor authorization disclosures containing the information required by the NPRM and the aforementioned complaint/dispute information that third parties and data aggregators can use to ensure compliance with the Section 1033 final rule. Such model disclosures should, in simple and plain language, explain to consumers how their data will be used and shared, as well as the controls available to the consumer. The Bureau may also consider whether a short form and long form disclosure approach is preferable so that the consumer is aware of the key facts and circumstances of their data sharing, with additional information being provided on a second, more complete disclosure document.

B. *Third Party Obligations – Certification Statement*

The Bureau should:

- ***Require third parties certify they will comply with third party obligations for all data accessed through a developer interface, rather than just covered data.***
- ***Mandate third parties certify their acceptance of liability in certain circumstances, and that they are adequately capitalized and carry sufficient indemnity insurance to fulfill their liability obligations.***

The certification statement provided as part of the authorization disclosure, in which the third party agrees to comply with their third party obligations under the statute, should specifically state the third party agrees to comply with such obligations in connection with *any* data accessed via the developer interface. As currently proposed, the certification statement requires a third party to certify it will comply with the third party obligations under proposed section 1033.421. As an initial matter, the Bureau should publish model disclosures well in advance of the effective date. The obligations contained in certification statement are only with respect to "covered data."[131] For example, proposed section 1033.421(a)(1) states: "[t]he third party will limit its collection, use, and retention of *covered data* to what is reasonably necessary to provide the consumer's requested product or service."[132] As drafted, these obligations would *not* apply to non-covered data that may be accessed through the developer interface. Third parties thus could access consumer data through the developer interface, but only a subset of that data – the "covered data" – would be afforded any protections regarding its collection, use, and retention. If data providers are able and elect to make both covered data and non-covered data available through the developer interface, then authorized third parties and data aggregators in the certification statement should certify they will comply with the obligations under section 1033.421 with respect to *any* data accessed through a developer interface. Section 1033.421 itself should also be revised to make it explicit that third party obligations apply to any data available

[131] 88 Fed. Reg. at 74873.
[132] *Id*. (emphasis added).

through a developer interface, covered data, and non-covered data alike. These obligations should apply to any data available through a developer interface regardless of how the third party or the data aggregator obtains the data. Absent such an obligation, third parties and data aggregators would be incentivized to engage in screen scraping to avoid these obligations.

As further described in Part VIII, the certification statements should also certify that: (i) third parties and data aggregators agree to accept potential liability for when consumer credentials are misused by a third party or data aggregator, or are compromised in a data breach then subsequently used to initiate a fraudulent transaction, and (ii) third parties and data aggregators are adequately capitalized and carry indemnity insurance to make good on their liability obligations.

C. *Third Party Obligations – Servicing or Processing*

The Bureau should provide a non-exhaustive list of activities that constitute permissible "servicing or processing."

The Bureau should provide specific examples of what activities constitute "servicing or processing" for purposes of proposed section 1033.421(c)(3). In outlining a third party's obligations vis-à-vis consumer's data, proposed section 1033.421 lists several examples of permissible uses of covered data, one of which is "servicing or processing the product or service the consumer requested."[133] It is not readily apparent what activities would constitute "servicing or processing" versus what activities would not be considered "reasonably necessary." As drafted, third parties will face significant uncertainty as to whether each specific use that is not required by law or to prevent fraud constitutes permissible "servicing or processing." Similar to the approach adopted by the Bureau in proposed section 1033.421(a)(2) – which outlines specific activities that are not part of, or reasonably necessary to provide, any other product or service – the Bureau in proposed section 1033.421(c)(3) should provide a non-exhaustive list of activities that constitute permissible "servicing or processing," as well as examples of activities that would *not* constitute permissible "servicing or processing."

D. *Third Party Obligations – Secondary Use Prohibitions*

The Bureau should prohibit reverse engineering confidential, proprietary information or other trade secrets.

The Bureau should revise proposed section 1033.421(b)(2) to state that reverse engineering a data provider's confidential, proprietary information or other trade secrets is a prohibited secondary use. This prohibition should apply regardless of whether or not the relevant data is deidentified. If third parties and data aggregators

[133] 88 Fed. Reg. at 74874.

are able to access consumer data through a data provider-funded developer interface, and then use that information to reverse engineer that data provider's trade secrets or other proprietary information, data providers will be disincentivized from sharing more information than minimally necessary through the developer interface.

Also, for purposes of proposed section 1033.421(b)(2), the Bureau should define reverse engineering to also include making analogous offers to consumers based on observation of the terms of credit accessed through a developer interface; alternatively, the Bureau could include this behavior as a separate prohibited secondary use under section 1033.421(b)(2). Allowing third parties to make offers to consumers that are equivalent to offers the consumer already has with their data providers based on observations and extrapolations made from the terms of credit accessed through those data providers' developer interfaces will lead to a stagnant, anticompetitive market, as parties will essentially be chasing the same end-state which will result in a decrease in the diversity of offers available to consumers. Such copycat practices would generally not clear any credit risk or other safety and soundness expectations for banks, but nonbanks are generally not subject to such regulations or related supervisory oversight. Particularly given the growth of nonbank credit – which the Bureau presumably seeks to further enable with this proposed rulemaking – it is possible that the aggregate risks of such copycat underwriting could raise financial stability concerns.

Failing to explicitly prohibit reverse engineering will also undermine the exception under proposed section 1033.221(a) for "confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors."[134] If third parties and data aggregators are permitted to reverse engineer confidential, proprietary information or trade secrets from data accessed through a developer interface, they will essentially have the power to access a data provider's "confidential commercial information" despite the proposed regulatory prohibition. This will result in an anticompetitive environment, which is the opposite outcome the Bureau seeks to achieve. Importantly, this restriction on reverse engineering would not impact consumers' ability to obtain consumer financial products and services from third parties, or the ability of third parties and data aggregators to facilitate the data access ecosystem and develop their own algorithms.

E. *Third Party Obligations – Secondary Use Definitions*

The Bureau should include definitions of "targeted advertising," "cross-selling of other products or services," "sale of covered data," and "consumer's requested product or service."

CBA recommends that the Bureau further define the specific prohibited activities under proposed section 1033.421(a)(2). Unlike banks, third parties and data aggregators

[134] *Id.* at 74870.

access to consumer data is predicated on one-time interactions. "Targeted advertising," "cross-selling," and "sale" could all have different meanings in different contexts and business models. Without clear definitions that take into account how third parties and data aggregators obtain permissioned data, they may use consumer data in ways unintended by consumers while mistakenly believing that the use is "reasonably necessary" to provide a consumer's requested service. In light of the fact that banks' practices with respect to covered data will be subject to additional regulatory obligations, including GLBA, any further definition of these terms should specifically detail prohibited data use practices for nonbanks, which are not subject to the same preexisting obligations for data use that banks already are subject to. It is also unclear under proposed section 1033.421(a)(2) what the Bureau means by "other" product or service, since proposed section 1033.421(a)(1) already limits secondary uses to what is reasonably necessary for providing a "consumer's requested product or service." It is not readily apparent as drafted what exactly the Bureau is referring to in proposed section 1033.421(a)(2) with the term "other product or service." Accordingly, the Bureau should clarify that this is a reference to the consumer's requested product or service from the third party. Absent clear rules and dedicated regulatory oversight, limitations on the ability of data aggregators and third parties to use consumers' data will lack accountability and enforcement.

The Bureau should also define the term "consumer's requested product or service." As proposed section 1033.421 is currently drafted, the limitations on third parties and data aggregators for use of consumer's data is fundamentally tied to what is "reasonably necessary to provide the consumer's requested product or service."[135] The scope of a "consumer's requested product or service" is not defined, yet this will have a tangible impact on whether any particular secondary use is permitted or not. The Bureau summarizes that it "will treat the product or service as the core function that the consumer sought in the market and that accrues to the consumer's benefit. For example, the scope of the product or service is not defined by disclosures, which could be used to create technical loopholes by expanding the scope of the product or service the consumer requested to include any activity the company chooses that would often benefit the third party and not the consumer."[136] This suggests the Bureau intends to decide on a case-by-case basis what the true scope of a "consumer's requested product or service" is, and then determine whether a use was "reasonably necessary' for providing that product or service. In the alternative, the Bureau may rely on whatever representations the third party makes, which would make this provision all but meaningless. This approach will generate significant uncertainty, as third parties and data aggregators will need to make determinations about whether certain uses are permissible in connection with a product that their own terms of service, under the Bureau's view, cannot create a properly defined scope for. Further, it is highly likely that entities that are closely supervised by the Bureau maintain a narrow definition,

[135] *Id*. at 74873.
[136] *Id*. at 74833.

while non-supervised third parties push the boundaries. Given the wide breadth of potential readings – and the critical importance of this vague provision – greater clarity by the Bureau is required.

As the Bureau provides more pragmatic guidance, the definition of a "consumer's requested product or service" should treat the "core" product or service the consumer is receiving as the "requested" product or service. A product being clearly and prominently described and marketed to a consumer is evidence that such product is the "core" product or service. In providing further clarity on the term "consumer's requested product or service," the Bureau should also indicate the extent to which the "standalone product" exception[137] will be evaluated and applicable to a "consumer's requested product or service." This clarification is necessary to ensure the availability and integrity of many market participants' standalone products offered to their consumers.

F. *Third Party and Data Aggregator GLBA Obligations*

The Bureau should clarify whether, and to what extent, the data use limitations contained in a Section 1033 final rule supersede any limitations that might exist on the use of that data under GLBA.

Industry would deeply benefit from the Bureau further clarifying how a party's obligations under GLBA intersect with the party's obligations under the Section 1033 final rule, particularly because in the data access ecosystem a single entity may function as a data provider in some instances, but an authorized third party in other instances. Director Chopra has stated publicly a desire to look at alternatives to longstanding GLBA privacy rules.[138] It is CBA's understanding that a Section 1033 final rule would not replace GLBA obligations. To the extent that limitations on data use under a Section 1033 final rule are narrower than those under GLBA, the Section 1033 final rule's limitations would control for the relevant data obtained through the developer interface. The Bureau should confirm whether this understanding is correct.

The NPRM does not further limit data providers' use of consumer data already in the data providers' systems beyond the limitations contained under GLBA or other applicable law. Data providers can thus engage in secondary use of data they already possess to the extent already permitted under GLBA. However, the NPRM indicates if an entity, which previously has operated as a data provider, is now acting as an authorized third party, the Section 1033 final rule's limitations on secondary use will apply to information that entity obtains from another data provider through the other data provider's developer interface. This will necessitate entities operating as both data

[137] *Id*. at 74833-34, fn. 130.
[138] Rohit Chopra, Dir., Consumer Fin. Prot. Bureau, *Prepared Remarks at Money 20/20* (Oct. 25, 2022), https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/.

providers and third parties – which in the Bureau's ideal framework, would likely be every data provider and third party – to build and develop systems to track whether data in their possession is subject to GLBA limitations or subject to Section 1033 limitations. By adding additional complexities to the existing ecosystem, the resources required to navigate that ecosystem necessarily increase. The time and costs are not sufficiently accounted for in the NPRM. The Bureau should explicitly clarify this for industry so all data access ecosystem participants can undertake the necessary steps to prepare.

VII. SSOs

The Bureau should:

- ***Revise the "openness" and "balance" prongs of the SSO-recognition process to acknowledge that data access ecosystem participants electing to not join an SSO does not mean that such SSO lacks "openness" or "balance."***
- ***Revise the "due process" and "transparency" prongs of the SSO-recognition process to protect anonymity of participant viewpoints and encourage open dialogue.***
- ***Treat compliance with an SSO's promulgated standards as sufficient, but not necessary, to establish compliance with the Section 1033 final rule.***

CBA applauds the Bureau for recognizing the importance of market-based standards for the data access ecosystem. As mentioned in Part I.b, CBA questions whether Section 1033's statutory language contemplated granting the Bureau the authority to impart special recognition to certain SSOs. Nevertheless, CBA urges the Bureau to ensure that SSOs continue to play a significant role. However, CBA recommends that the Bureau reconsider several aspects of the treatment of SSOs under the NPRM. As a threshold matter, the Bureau should reconsider its approach to recognizing SSOs. For many components of the rule, indicia of compliance includes conformance with standards promulgated by fair, open, and inclusive standard-setting bodies recognized by the Bureau.[139] The final rule should make clear that the SSO is free to determine appropriate standards as it sees fit, without out further CFPB approval or oversight, once recognized. An SSO is "fair, open, and inclusive" when it has seven specific attributes: (i) openness, (ii) balance, (iii) due process, (iv) appeals, (v) consensus, (vi) transparency, and (vii) Bureau recognition.[140] Several of these prongs need to be reconsidered in evaluating whether a SSO is "fair, open, and inclusive." The "openness" prong evaluates whether "sources and processes used are open to all interested parties, including consumer and other public interest groups, authorized third parties, data providers, and data aggregators,"[141] while the "balance" prong considers whether "decision-making power is balanced across all interested parties, including consumer

[139] 88 Fed. Reg. at 74801.
[140] *Id.* at 74869.
[141] *Id.*

and other public interest groups, with no single interest dominating decision-making."[142] These two prongs taken together suggest the Bureau is looking for an SSO with an expansive, broad membership in which all members are deeply involved in standard development.

However, an overly expansive membership has the potential to result in the standard-development and approval process becoming unwieldy. It is unlikely that a single SSO will be able to promulgate standards that satisfies its entire membership if the membership composition is so expansive and diverse. As such, the Bureau should recognize that an SSO not having every potentially interested party in its membership does not mean the SSO lacks "openness" or "balance." In fact, just because an SSO is open to all parties joining does not actually mean all interested parties will join. Parties may decline to join an SSO for a variety of reasons. These parties being offered opportunities on the same terms as others but choosing not to join an SSO should not be held against the SSO when it applies to the Bureau for recognition. To address this concern, the "openness" prong should be reframed to ensure that interested parties have the opportunity to join membership, and that all members, rather than all interested parties, have access to sources and processes. Similarly, the "balance" prong should be reframed to consider whether decision-making power is balanced across all members, not all interested parties.

The Bureau should also clarify that the "transparency" prong, which would require that "[p]rocedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available,"[143] not necessitate the sharing of any confidential, proprietary, or competitive information of an SSO's members. It is likely that many potential SSO members would be less inclined to assist in the development if their sensitive information were to be shared, which would impact the number of voices involved in creating the best standards for the overall data access ecosystem. Similarly, the "due process" prong would require that the SSO makes "access to views and objections of other participants" available. While a diversity of opinions is important to the formation of standards, full transparency into all internal discussions could perversely curtail the open dialogue necessary for standard development and, much like the aforementioned implications of the "transparency" prong, actually disincentivize participation. Any publicly available "access to views and objections of other participants" should at least be aggregated and summarized to protect the anonymity of individual participants.

Additionally, industry will face significant compliance hurdles, increased costs, and less standardization with consumer-friendly protocols if no standards promulgated by a fair, open, and inclusive standard-setting body are recognized by the Bureau as of the dates for compliance with the final rule. In the absence of a recognized SSO, data providers

[142] *Id.*
[143] *Id.*

would essentially be required to build their systems to come into compliance with wholly unidentified standards, taking their best guess as to what will be needed from their systems. The NPRM states that data providers would be compliant in such instances by "meet[ing] the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers."[144] It is wholly insufficient to build a durable and efficient data access system by encouraging data providers to do their best to copy the efforts of other data providers, particularly when there is no standard provided that industry knows they should build their systems toward to be compliant with the Section 1033 final rule and virtually no lead time to effectively plan and manage updates.

The Bureau can mitigate some of these concerns by independently recognizing a currently-existing SSO as maintaining standards industry can build their systems toward in order to achieve compliance. Recognizing a currently-existing SSO would minimize disruption to the data sharing ecosystem, as many data providers would already be aware of such an SSO and familiar with the standards it has promulgated. Importantly, it appears that under the NPRM the Bureau has the authority to designate an SSO as an issuer of qualified industry standards without the SSO necessarily having applied to the Bureau for recognition. Proposed section 1033.141(b) states "[a] standard-setting body *may* request that the CFPB recognize it as an issuer of qualified industry standards."[145] Nothing in this language suggests that it is a necessary precondition that the SSO have requested the Bureau recognize it as an issuer of qualified industry standards before the Bureau actually does so. This nuance affords the Bureau the opportunity to quickly and preemptively identify an SSO as an issuer of qualified industry standards that data providers can build their systems to be compliant with. Such SSO could also be identified simultaneously with issuance of the final rule. To that end, after the publication of the Section 1033 final rule, the Bureau should make available to industry a continually updated list of recognized SSOs whose standards data providers can comply with. The website should also include information on how to apply to become an SSO, ways to provide notice and comment to pending applications, and copies of any denials that include specific reasons for denials, and protocols for appeals of any initial decisions. Including this information would align the Bureau with its own expectations for requirements of the SSOs. This will continue to foster the development of the data access ecosystem by providing clear standards that data providers can aim to build toward, particularly as technology advances and standards issued by SSOs may change over time.

It is vital though that, regardless of when or how many SSOs the Bureau recognizes, compliance with an SSO's promulgated standards be treated as sufficient, *but not necessary*, for demonstrating compliance with a data provider's obligations under the Section 1033 final rule. As the data access ecosystem evolves, the Bureau may recognize

[144] *Id*. at 74871.
[145] *Id*. at 74870 (emphasis added).

different SSOs, and the standards promulgated by these SSOs will change. If new standards are established through the SSO, the SSO should also be able to provide recommended timelines for updates or provide a sufficient runway prior to the updated standards being effective. Data providers' systems may continue to meet the high levels of quality and assurance that they met under a former standard that has slightly changed, yet the rule would suggest that a data provider in such instance would be noncompliant with the Section 1033 final rule. While data providers should be able to demonstrate compliance with the final rule by complying with a recognized SSO's standards, this should not be the only avenue available to data providers to demonstrate compliance. Data providers should be permitted to demonstrate to the Bureau that their systems meet a "reasonable" standard, even if such standard does not exactly match one promulgated by an SSO. This flexibility is necessary for several reasons. First, it may be difficult for an SSO to reach a consensus agreement on some particular standard elements given the potential diversity of viewpoints that will be necessary for the SSO to be recognized by the Bureau. In these instances, even if an SSO has not promulgated a standard on a specific topic, a data provider may still be acting "reasonably" in compliance with the rule with respect to how the data provider has built their system and should be able to demonstrate as much. Second, some elements may not necessarily be suited to standardization by an SSO. For example, policies and procedures may need to be tailored to each specific data provider, their business model, and the current regulatory landscape. These policies and procedures may be reasonable and compliant with the Section 1033 final rule even if they do not match exactly what may have been previously promulgated by an SSO. Further, if there are multiple SSOs, there may be a conflict as to one specific standard, which would be resolved by adopting the approach discussed above. Treating SSO standards as akin to "recommended practices" that can demonstrate compliance with the rule, rather than as strict requirements that must be adhered to in order to be compliant, will prevent data providers from being held as noncompliant for implementing systems that differ from, but are no less protective or effective than, SSO standards. In fact, some of the differences may result from the speed with which data providers adapt to technological or regulatory developments. Data providers should not be disincentivized from efficiency by the risk of being deemed noncompliant with the rule.

VIII. Liability

The Bureau should:

- ***Explicitly state liability rests with the responsible third party or data aggregator if a consumer's credentials are misused to initiate a fraudulent transaction by such party or are impermissibly acquired by another actor through a data breach the party experienced.***
- ***Mandate third parties and data aggregators be adequately capitalized and carry sufficient indemnity insurance to satisfy liability obligations.***

- ***Obligate third parties to certify as part of the certification statement that they are adequately capitalized, have accepted their liability obligations, and are carrying sufficient indemnity insurance.***

The NPRM presupposes that existing liability frameworks, specifically Regulation E, and bilateral contracts, will adequately allocate liability among data access ecosystem parties.[146] These methods are inadequate for meaningfully allocating liability under the NPRM's data sharing framework. Liability may eventually rest with the consumer or with the data provider even though a data aggregator or third party was responsible for a breach that compromised a consumer's covered data, which may then have been used to initiate a fraudulent transaction. The Bureau should explore alternatives that will place appropriate liability on third parties and data aggregators to ensure that risks and costs are appropriately allocated and shared among all market participants. Absent cost sharing, third parties and other downstream entities may not have sufficient motivation to invest in data security standards, putting consumer data at increased risk. These alternatives can include requiring third parties and their data aggregators to carry insurance, and specifying instances in which a third party or data aggregator failing to comply with a consumer request would alleviate a data provider of liability for subsequent unauthorized transactions.

Current protections under Regulation E and Regulation Z do not sufficiently map on to the parties with the greatest ability to prevent unauthorized transactions in the data access ecosystem. Under current regulatory provisions, liability would appear to rest with a data provider or with a consumer, even if a third party or a data aggregator misused the consumer's covered data or suffered a breach resulting in the disclosure of a consumer's covered data, that was then used to effectuate an unauthorized transaction. As further detailed in Part III.c of this letter, compromised credentials can be used to initiate fraudulent transactions. If disputed under Regulation E, the consumer can only be reimbursed for the transactions that occurred up to and until 60 days after receipt of the periodic statement listing the first unauthorized transaction. If the consumer notifies the data provider in a timely manner, an investigation will be undertaken by the financial institution. Based on the findings, either the consumer will accept the loss, or the financial institution will credit the consumer.[147] If the NACHA Rules apply, the consumer generally has a longer window to dispute a transaction.[148] In no point in this dispute and review process can a third party or data aggregator be held liable, even if they are the source of how the credentials were compromised. Moreover, there are

[146] *See, e.g.*, *id.* at 74801 ("Consumers are protected from liability from these unauthorized transfers under EFTA and Regulation E, although the relevant financial institution may be able to seek reimbursement from other parties through private network rules, contracts, and commercial law. For example, although a consumer's financial institution is required to reimburse the consumer for an unauthorized transfer under Regulation E, ACH private network rules generally dictate that the receiving financial institution is entitled to reimbursement from the originating depository institution that initiated the unauthorized payment.").
[147] *See generally* 12 C.F.R. § 1005.11.
[148] *See* Part III.c.

circumstances under which a consumer will be held liable for fraudulent transactions, such as when a consumer fails to report a fraudulent transaction within the allotted timeframe[149] or when an agent of the consumer has exceeded the scope of their authorization.[150]

Existing bilateral contracts are insufficient for addressing liability under the new data access ecosystem that would exist following the Section 1033 final rule. While many bilateral contracts today address liability, these contracts often contain limitations on liability and may not cover liability for downstream parties that receive information from the third party or data aggregator. Enforcing the terms of the contracts, to the extent there are disagreements between the parties, can be costly and time consuming. Bilateral contracts today are usually extensively negotiated, and thus not an effective method for establishing consistent consumer protection. Moreover, reliance on bilateral contracts ignores the market reality that the largest third parties and data aggregators are able to more effectively limit their liability as part of the contract negotiation process. Additionally, third parties and data aggregators will more meaningfully engage with and invest in their data security obligations under the Section 1033 final rule if these parties have a financial incentive to prioritize their data security due to the risk of liability. Simply put, any party in the data access ecosystem will be more likely to rigorously protect consumers' data if there is a chance that party could be held liable for the eventual misuse of that data.

To address this circumstance, the Bureau should require third parties and data aggregators to include in their certification statement, as a condition of accessing the developer interface, that neither data providers nor consumers are liable for any action or inaction by a third party or a data aggregator that compromises a consumer's data. This includes a consumer's credentials, which are then used to initiate a fraudulent transaction, including a data breach of said third party or data aggregator. Instead, in these instances the third parties and data aggregators are certifying that liability should rest with them, independent of background liability frameworks set out in relevant regulation or law, because they were the party in the best position to prevent the harm to the consumer. Indeed, data aggregators may have access to more information than any other party in the data access ecosystem, yet under the NPRM appear to have the least obligations. It is very important that data aggregators, and not just third parties, have potential liability to ensure consumers' data is meaningfully safeguarded by all data access ecosystem participants, and that consumers have sufficient assurances that responsible parties will make them whole for any losses. To ensure compliance with these proposals, the Bureau must require that all third parties and, if applicable, data aggregators, as part of the certification statement, certify that they will accept liability in

[149] *See generally* 12 C.F.R. § 1005.6.

[150] 12 C.F.R. Part 1005, Supp. I, cmt. 2(m)-2 ("If a consumer furnishes an access device and grants authority to make transfers to a person (such as a family member or co-worker) who exceeds the authority given, the consumer is fully liable for the transfers unless the consumer has notified the financial institution that transfers by that person are no longer authorized.").

such instances. Whether there are agreements between an authorized third party and a data aggregator, the parties should be joint and severely liable, to further incentivize third party due diligence and market driven risk management. To the extent the Bureau has supervisory authority over these entities, the Bureau should examine these third parties and data aggregators to ensure they have complied with their obligations to assume liability.[151] This includes use of the Bureau's broad authority to examine nonbanks whose activities the Bureau has reasonable cause to determine pose risks to consumers under Section 1024(a)(1)(C) of the Dodd-Frank Act. If the Bureau lacks supervisory authority over a data aggregator or third party, the Bureau should engage with the relevant regulatory authority to ensure these entities are compliant with the Section 1033 final rule.

The possibility of liability resting with third parties and data aggregators is not enough to protect consumers. In some instances, even if liability does rest with a third party or data aggregator, that third party or data aggregator may not be financially viable for consumers to meaningfully have recourse options against it. Just because the entity is liable does not mean the entity will be capable of making consumers whole. To address this circumstance, the Bureau should require that third parties and data aggregators, in addition to having liability to the consumer in certain circumstances, be adequately capitalized and carry sufficient indemnity insurance to make good on their liability obligations. The failure of a third party or data aggregator to accept these liability obligations, be adequately capitalized, and carry indemnity insurance should be a reasonable basis for a data provider to deny access to the developer interface. The Bureau should not allow parties denied access for such reasons to attempt to screen scrape the same data. The final rule should require that the third party and the data aggregator, as applicable, provide the data provider with information about the acceptance of liability and confirmation of adequate capitalization and appropriate indemnity insurance that can be independently verified as part of the certification statement. Moreover, it is vital that all parties in the data access ecosystem be aware of these obligations and representations. This information should also be made publicly available on the authorized third party and data aggregator's website, to the extent they have a digital presence.

It is surprising that, given the various parts of the NPRM directly based on the implementation of open banking in other jurisdictions,[152] the Bureau declined to incorporate these jurisdictions' approaches to liability. These approaches are a key part of the ecosystem operating effectively, allocating risks appropriately, and reducing safety and soundness concerns for financial institutions. For example, under PSD2 third party service providers are required to hold a professional indemnity insurance

[151] The Bureau should also use its authority under 12 U.S.C. § 5516(e) to supervise authorized third parties and data aggregators that provide services to a substantial number of persons as described in 12 U.S.C. § 5516(a).
[152] *See, e.g.*, 88 Fed. Reg. at 74816.

that covers all territories they operate in.[153] The Payment Services Regulation 2017 in the United Kingdom explicitly acknowledges the importance of these third parties holding insurance to make consumers whole in the event of financial harm:

> *Payment initiation service providers and account information service providers, when exclusively providing those services, do not hold client funds. Accordingly, it would be disproportionate to impose own funds requirements on those new market players. Nevertheless, it is important that they be able to meet their liabilities in relation to their activities. They should therefore be required to hold either professional indemnity insurance or a comparable guarantee. EBA should develop guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 on the criteria to be used by Member States to establish the minimum monetary amount of professional indemnity insurance or comparable guarantee. EBA should not differentiate between professional indemnity insurance and a comparable guarantee, as they should be interchangeable.*[154]

Similarly, Canada has proposed a liability regime that rests on the premise that liability should flow with the data and rests with the party at fault.[155] In order to meaningfully protect consumers, the Bureau should similarly require third parties and data aggregators be adequately capitalized and hold indemnity insurance. The fact that third parties and data aggregators are adequately capitalized and required to maintain such insurance to make consumers whole should also be noted in any disclosures by the third party or data aggregator to the consumer. Most consumers may initially otherwise believe their data provider is the only party liable for unauthorized transactions resulting from a third party data breach.

The allocation of liability in the Section 1033 final rule should be guided by the principle that the party responsible and in the best position to prevent the harm to the consumer is liable. For example, if an authorized third party fails to comply with a consumer's request to revoke authorization or fails to communicate such revocation to its data aggregator, the data provider should not bear liability. Instead, liability should rest with the third party, which was in the best position to prevent harm to the consumer. Similarly, when more information is accessed than necessary to offer a particular product or service, the liability should rest with the third party or data aggregator that is

---

[153] *See* Deloitte, *PSD2 – Payment Services Directive 2: What is new?*, https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/psd2-revised-payment-services-directive.html.

[154] The Payment Services Regulations 2017(SI 2017/752), https://www.legislation.gov.uk/uksi/2017/752/pdfs/uksi_20170752_en.pdf.

[155] Advisory Committee on Open Banking, Department of Finance Canada, *Final Report – Advisory Committee on Open Banking* p. 16 (Apr. 2021), https://www.canada.ca/content/dam/fin/consultations/2021/acob-ccsbo-eng.pdf.

accessing the additional information, rather than the data provider that, to its knowledge, is complying with a valid request from a third party or data aggregator.

IX. Compliance Timeframes

The Bureau should adopt a two-track compliance timeline based on whether the Bureau has recognized a standard-setting body as an issuer of qualified industry standard.

The staggered compliance dates outlined in proposed section 1033.121 – which would afford the largest institutions only six months after publication of the final rule in the Federal Register to comply but grant the smallest depository institutions four years to comply[156] – are wholly unreasonable and untenable in light of both the work that will need to be undertaken by data providers, and the fact that data providers may not even know what standards they should build their developer interfaces to comply with in the absence of a standard promulgated by a Bureau-recognized SSO while also being impossible to otherwise start work prior to the issuance of any final rule. The changes proposed in the NPRM are tantamount to a sea change to the entire data sharing ecosystem, not minor refinements.

The Bureau's required first compliance date of six months after publication of the final rule in the Federal Register for depository institutions holding at least $500 billion in total assets and nondepository institutions generating or projected to generate at least $10 billion in revenue is unreasonably short. All data providers, regardless of size, will be engaged in substantial work, or reworking, of their developer interfaces to comply with the Section 1033 final rule. As CBA summarized in its comments on the SBREFA Outline:

> *The Bureau significantly underestimates the ease with which a third-party access portal can be developed and implemented by data providers. Many data providers, small and large alike, do not currently have an application programming interface (API) that could provide consumer information, especially to the extent currently under consideration, to authorized third parties. Developing an API from the ground up is costly and would pose a significant financial burden on many data providers. Moreover, data providers that seek to enter strategic partnerships to build out an API would need, at a minimum and under the best circumstances, at least 12 months. Even for data providers that already have a third-party access portal, the cost of maintenance would skyrocket to support the proposals… Each of these changes in isolation would impose significant costs on data providers that already*

[156] 88 Fed. Reg. at 74869.

utilize APIs; these potential changes in the aggregate would impose overwhelming costs.[157]

Moreover, in proposing the compliance timelines in the NPRM, the Bureau has failed to account for the fact that third parties and data aggregators will also be engaging with these developer interfaces for the first time and will need to adapt their practices to be compliant with the final rule and to avoid interruptions to existing products or services. Failing (i) to afford data providers adequate time to ensure they can develop and maintain developer interfaces that are compliant with the Section 1033 final rule, and (ii) to provide third parties and data aggregators sufficient time to prepare to interface with these new developer interfaces, is likely to result in increased disruptions and difficulties, significant burdens on market participants, and increased risk of unintended consequences from a rushed process. The Bureau can mitigate the severity of these initial stumbling blocks in the post-Section 1033 final rule data access ecosystem by providing all parties enough time to develop and test system engagement.

In light of the foregoing, CBA urges the Bureau to shift away from the compliance timeframes outlined in the NPRM and instead adopt a two-track compliance timeline based on whether the CFPB has recognized a standard-setting body as an issuer of qualified industry standards:

- If the Bureau *has not* officially recognized at least one standard-setting body as an issuer of qualified industry standards at the time the final rule is published in the Federal Register, the largest data providers should have a minimum of 24 months to come into compliance from the date of publication.
- If the Bureau *has* officially recognized at least one standard-setting body as an issuer of qualified industry standards at the time the final rule is published in the Federal Register, the largest data providers should have a minimum of 12 months, but preferably 18 months, to come into compliance from the date of publication.

This approach will increase the chances that all industry participants will have sufficient time to come into compliance with either standards that are known to those in the market or, if no such approved standards have been recognized by the Bureau, to determine a set of standards that industry should collectively build toward. Additionally, in light of the considerations in Part X, the Bureau should strongly consider aligning the compliance dates for data providers under Section 1033 with the compliance dates of other relevant rulemakings, including the FCRA rulemaking.

---

[157] 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), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

X. Additional Considerations

The Bureau should:

- ***Clarify whether virtual currencies are "funds" for purposes of determining whether nonbanks offering virtual currencies fall within the scope of "data providers."***
- ***State that a data provider complying with obligations under the Section 1033 final rule does not make that data provider a "furnisher" under the FCRA.***
- ***Provide further information on how the obligations under the Section 1033 final rule intersect with those under the Bureau's 1034(c) AO.***
- ***Identify what exact activities, if undertaken, would result in a data aggregator being classified as a "consumer reporting agency" under the FCRA.***

CBA wishes to raise two process-related considerations in connection with this NPRM for the Bureau's consideration. First, CBA urges the Bureau to thoughtfully consider how this NPRM and a final Section 1033 rule will intersect with other ongoing rulemaking efforts by the Bureau, specifically the Bureau's ongoing rulemaking to supervise larger nonbank participants in the market for general-use digital consumer payment applications[158] (LPR rulemaking on consumer payment apps), and the forthcoming rulemaking on consumer reporting[159] (FCRA rulemaking). It is vital that the Bureau engage in intelligent notice-and-comment rulemaking so it can obtain meaningful feedback on these concurrent rulemaking efforts with substantial cross-effects.

As a result of the Bureau's rulemaking on consumer payment apps, some nonbanks may be "data providers" and subject to obligations under a Section 1033 rule that are not immediately apparent when reviewing the LPR rulemaking on consumer payment apps in isolation. In the LPR rulemaking on consumer payment apps, the Bureau proposes to clarify that virtual currencies are "funds" under the Consumer Financial Protection Act (CFPA).[160] It is unclear whether the Bureau has concluded that the same definition would apply to the use of the term "funds" in the Electronic Fund Transfer Act (EFTA),[161] a topic the Bureau expressly declined to opine on in the LPR rulemaking on consumer payment apps: "*Without fully addressing the scope of that term,* the CFPB

---

[158] Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, 88 Fed. Reg. 80197 (Nov. 17, 2023).

[159] On September 15, 2023 the Bureau issued a SBREFA outline for a consumer reporting rulemaking. Comments on the SBREFA outline were due by October 30, 2023, although some entities were permitted to submit comments by November 6, 2023. *See* CFPB, *Small Business Advisory Review Panel for Consumer Reporting Rulemaking – Outline of Proposals and Alternatives under Consideration* (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.

[160] Public Law 111-203, 124 Stat. 1376, 1955 (2010).

[161] 15 U.S.C. 1693 *et seq.*, implemented by Regulation E, 12 C.F.R. part 1005.

believes that, consistent with its plain meaning, the term 'funds' in the CFPA is not limited to fiat currency or legal tender, and includes digital assets that have monetary value and are readily useable for financial purposes, including as a medium of exchange. Crypto-assets, sometimes referred to as virtual currency, are one such type of digital asset."[162] If virtual currencies are "funds" under both the CFPA and EFTA, then there may be nonbanks offering virtual currencies that are also offering Regulation E accounts, and thus would fall within the scope of "data providers" under a Section 1033 final rule. CBA in this letter does not opine on the appropriateness of the definition of "funds" under CFPA and EFTA, nor on the implications this has for nonbanks that may be "data providers," but cautions the Bureau that this is a matter that requires further attention and exploration.

Industry has similarly warned about cross-effects in connection with the FCRA rulemaking that similarly need to be further evaluated.[163] Industry has warned that the regulatory changes that would be contemplated in the FCRA rulemaking could compound banks' burdens under a Section 1033 rule. The proposals in the SBREFA outline for the FCRA rulemaking would significantly expand the definition of "consumer reporting agency."[164] As a result banks may be routinely forced to "furnish" consumer information to consumer reporting agencies and face significant additional compliance burdens and liabilities under the Fair Credit Reporting Act. CBA recommends that the Section 1033 final rule clarify that a data provider complying with their obligations under such final rule does not make it a "furnisher" under the FCRA. If the Bureau does not address this issue in the Section 1033 final rule, then it should be clarified in the FCRA rulemaking that a data provider sharing data at a consumer's direction pursuant to Section 1033 is not "furnishing" information under the FCRA. Further, so all data access ecosystem participants are aware of their obligations under both the Section 1033 final rule and the FCRA rulemaking, the Bureau should identify the exact activities that, if undertaken, would result in a data aggregator being classified as a "consumer reporting agency" under the FCRA. Given the significant intersections between the Section 1033 rulemaking and the FCRA rulemaking, the Bureau should consider not requiring compliance with the Section 1033 final rule until after the FCRA rulemaking is finalized, so parties are fully aware of the totality of their obligations under the new data access ecosystem. In light of how significant of an overlap there may be between parties subject to obligations under both the Section 1033 final rule and the FCRA rulemaking,

---

[162] Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, 88 Fed. Reg. 80197, 80202 (Nov. 17, 2023) (emphasis added).
[163] *See, e.g.*, Bank Policy Institute et al., *Comments on the Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration* (Nov. 6, 2023), https://www.consumerbankers.com/sites/default/files/BPI%20CBA%20TCH%20Comment%20on%20CFPB%20SBREFA%20Outline%20for%20Rulemaking%20on%20FCRA.pdf.
[164] *See generally*, Consumer Financial Protection Bureau, *Small Business Advisory Review Panel for Consumer Reporting Rulemaking – Outline of Proposals and Alternatives under Consideration* 6-12 (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.

the Bureau should strongly consider not requiring parties to comply with their obligations under the Section 1033 final rule until the FCRA rulemaking is finalized, so that market participants may holistically understand their obligations and develop their systems with an understanding of the full suite of their obligations.

Similarly, although not a formal rulemaking, the Bureau should clarify the extent to which the obligations under the Section 1033 final rule would intersect with the 1034(c) AO. The 1034(c) AO generally requires banks and credit unions to comply with a consumer's request for information about the consumer financial product or service the consumer is obtaining from the bank or credit union; the 1034(c) AO further specifies that imposing conditions that "unreasonably impede consumers' information requests" would be a violation of the obligation to "comply," and one action that would "unreasonably impede consumers' information requests" would be requiring a consumer to pay a fee or charge to request this information.[165] Although the Bureau acknowledges that the 1034(c) AO does not preempt or supersede a Section 1033 final rule,[166] the Bureau should clarify to what extent the scope of data covered by Section 1033 and by the 1034(c) AO overlap, and how that may impact obligations for data providers.

The foregoing matters, in conjunction with the other issues raised in this comment letter, are very complex issues that require time and effort to evaluate. To properly evaluate these issues, a longer comment period should have been afforded to commenters by the Bureau. Fifteen trade associations submitted a joint comment letter[167] to the Bureau on October 27, 2023 requesting that the Bureau extend the comment period from 71 days[168] to 90 days after publication of the NPRM in the Federal Register. This request was supported by the U.S. Small Business Administration Office of Advocacy,[169] yet was not granted by the Bureau. This decision by the Bureau is particularly puzzling in light of the fact that each of the prior comment periods for

---

[165] Consumer Information Requests to Large Banks and Credit Unions, 88 Fed. Reg. 71281, fn. 27 (Oct. 16, 2023) ("Relatedly, the CFPB does not interpret section 1034(c) to preempt or otherwise supersede the requirements of other Federal or state laws and regulations designed to protect privacy and data security. This includes, for example, any restrictions that may be imposed in the CFPB's upcoming rule implementing section 1033.").

[166] *Id*. at 71281.

[167] American Fintech Council et al., *Docket No. CFPB-2023-0052 – Request for Extension of Comment Period for Notice of Proposed Rulemaking on Personal Financial Data Rights* (Oct. 27, 2023), https://www.consumerbankers.com/sites/default/files/AFC%20Joint%20Trade%201033%20Comment%20Period%20Extension%20Request%2010.27.23.pdf.

[168] The NPRM was first posted online on October 19, 2023, but was not published in the Federal Register until October 31, 2023.

[169] U.S. Small Business Administration Office of Advocacy, *Request for Extension of the Deadline to File Comments to the Notice of Proposed Rulemaking on Personal Data Rights Docket No. CFPB-2023-0052 or RIN 3170-AA78* (Nov. 8, 2023), https://advocacy.sba.gov/wp-content/uploads/2023/11/Comment-Letter-CFPB-1033-Extension-of-Comment-Period.pdf.

Section 1033 offered at least 90 days.[170] It was misguided by the Bureau to fail to provide an extension of the comment period, particularly at the most crucial juncture in the Section 1033 rulemaking process thus far.

* * *

CBA values the opportunity to comment on this NPRM and appreciates that the Bureau has incorporated several recommendations from industry comments on the SBREFA outline into this NPRM. CBA hopes that the Bureau will thoughtfully consider and publish a final rule that is meaningfully informed by the recommendations in this comment letter. CBA remains available to meet with the Bureau to discuss any of the issues discussed in this letter and develop solutions that will ensure a tenable and viable Section 1033 final rule.

Sincerely,

Brian Fritzsche
Vice President, Associate General Counsel
Consumer Bankers Association

[170] The Bureau's original Request for Information published in the Federal Register on November 22, 2016, and Advance Notice of Proposed Rulemaking published in the Federal Register on November 6, 2020 both provided approximately 90 days for public comment. The SBREFA outline, issued on October 27, 2022, provided approximately 90 days for public comment.