January 25, 2023

Via Electronic Mail

Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20052
Financial_Data_Rights_SBREFA@cfpb.gov

Re: Feedback on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights - Outline of Proposals and Alternatives under Considerations

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) Small Business Regulatory Enforcement Fairness Act (SBREFA) outline[2] concerning consumers' personal financial data rights and the pending rulemaking pursuant to Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).[3] 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*."[4] Such information is to "be made available *in an electronic form usable by consumers*."[5]

In general, CBA strongly believes it is imperative that a final rule implementing Section 1033 (i) regulates all participants in the data ecosystem on a level playing field, (ii) prioritizes data security, (iii) protects consumer privacy, and (iv) establishes a clear liability standard. These principles should inform any final Section 1033 rule as follows:

- ***Level Playing Field***: The Section 1033 rule must include Bureau supervision of data aggregators.

[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] CFPB, *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights - Outline of Proposals and Alternatives under Consideration* (Oct. 27, 2022), *available at* https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.
[3] 12 U.S.C. § 5533.
[4] *Id*. (emphasis added).
[5] *Id*. (emphasis added).

- ***Data Security***: Many nonbank third parties and data aggregators are not subject to the same data security and privacy standards as banks, including normal course of business examinations by a Federal agency, which leaves consumer data exposed to potential bad actors when it leaves a regulated and supervised financial institution. A Section 1033 rule should ensure that all participants in the data access ecosystem that hold or process consumer financial data are held to the same, or materially comparable standards as those provided under the Gramm-Leach-Bliley Act (GLBA)[6] and its implementing regulations.[7] Moreover, the financial services industry, through industry standard-setting bodies such as the Financial Data Exchange (FDX), should continue to take the lead in developing the standards for consumer-authorized data access. Such an approach is the most efficient way to facilitate both innovation and interoperability.
- ***Privacy:*** Consumers should have full awareness and control over how their data is shared and used. Currently, when consumers share their data with nonbank third parties for a specific purpose, they do not know if or how their data is used beyond that intended purpose. Some nonbank third parties rely on screen scraping techniques to access data, which decreases consumer control over their data and is a fundamentally unsafe method of access and should be sunsetted. Consumers also commonly mistake deleting a mobile phone or computer application with revoking consent. As a result, nonbank third parties maintain continued, unfettered access to consumer information even after a consumer intends for the relationship to be terminated. To promote consumer control of their data security and privacy, a Section 1033 rule should require that consumers receive disclosures from nonbank third parties and data aggregators that explicitly communicate to consumers about any secondary or downstream use of their data and how consumers can revoke consent to use their data.
- ***Clear Liability:*** A Section 1033 rule must establish a clear liability standard for all parties in the data access ecosystem, and liability for consumer recourse should be imposed on the party that was in control of the consumer's data at the time of the breach or action.

CBA also notes that the plain statutory language of Section 1033 is fundamentally centered on a consumer's right to control their own information, regardless of whether a bank or a nonbank is a "covered person" holding that information; the language of Section 1033 is not narrowly focused on just the ability "for individuals to fire, or walk away from, their financial provider for whatever reasons"[8] in connection with only deposit accounts or credit card accounts. It is vital that a rule implementing Section 1033 reflects the broad applicability of the statutory text to apply equally to banks and nonbanks that hold consumer accounts and is clear about whether the obligations contained therein are account-specific or consumer-specific.

In the SBREFA outline, the Bureau solicits feedback on 149 specific questions. In addition to the general comments proffered in this letter, CBA is sharing more specific comments with the Bureau in response to the following questions.

---

[6] Public Law 106-102, 138Stat. 1338 (1999) (codified at 15 U.S.C. 6801 *et seq.*).
[7] 12 CFR Part 1016 - Privacy of Consumer Financial Information (Regulation P).
[8] Director Chopra's Prepared Remarks at Money 20/20 (Oct. 25, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/.

Q4. Please provide input on any costs or challenges you foresee with the enforcement or supervision of the proposals under consideration. In particular, please provide input on whether enforcement or supervision of the proposals under consideration may be impractical in certain circumstances and how the CFPB could address those concerns.

To fulfill the Bureau's mission of ensuring "Federal consumer financial law is enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition,"[9] the Bureau supervises and examines covered persons. However, while banks and credit unions are supervised and examined by the Bureau, other nonbank market participants are not subject to the same level of oversight. Nonbanks are increasingly providing financial products and services, yet their activities are largely unsupervised by the Bureau. According to the Federal Reserve Bank of New York, "fintechs" and nonbanks now issue nearly three-quarters of all unsecured personal loans.[10] In a November 2022 report, the U.S. Department of the Treasury noted that, "[n]ew entrant nonbank firms have a growing presence across core consumer finance markets and are increasingly managing the points through which consumers access financial products and services. This trend has been particularly acute in the markets for payments and consumer lending. The available data support the view that while entering core consumer finance markets via a bank charter remains limited, fintech firms have been entering the market in increasing numbers. Over 1,200 fintech firms, focused on consumer deposits, lending, and payments, formed in the decade following the 2007-08 global financial crisis."[11]

The Bureau does not adequately oversee these nonbank participants, even though they compose a significant, continuously growing segment of the market for consumer financial products and services. At present, the Bureau only has supervisory and enforcement authority over banks and a narrow set of nonbanks.[12] The U.S. Department of Treasury in its November 2022 report specifically signaled its concern about supervision of data aggregators, noting that "many data holders…can be subject to supervision and regulatory enforcement of their obligations regarding information security. On the other hand, data aggregators and data users are a more diverse

---

[9] 12 U.S.C. § 5511(b)(4).

[10] Eldar Beiseitov, *The Role of Fintech in Unsecured Consumer Lending to Low- and Moderate-Income Individuals - How Fintech Has Changed Access to Unsecured Consumer Loans*, Federal Reserve Bank of New York (Sept. 29, 2022), *available at* https://www.newyorkfed.org/medialibrary/media/newsevents/events/regional_outreach/2022/092922/2022-09-29-eldar-beiseitov-fintech-personal-loans-ny-fed.

[11] U.S. Dep't of Treasury, *U.S. Department of the Treasury Report to the White House Competition Council - Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets* 3 (Nov. 2022), *available at* https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf.

[12] The Bureau has supervisory authority over the following nondepository covered persons: (i) nonbanks offering or providing origination, brokerage, or servicing of loans secured by real estate for use by consumers primarily for personal, family, or household purposes, or loan modification or foreclosure relief services in connection with such loans; (ii) is a larger participant of a market for other consumer financial products or services, as defined by rule; (iii) nondepositories which the Bureau has reasonable cause to determine, by order, after notice to the covered person and a reasonable opportunity for such covered person to respond, based on collected complaints, that such covered person is engaging, or has engaged, in conduct that poses risks to consumers with regard to the offering or provision of consumer financial products or services; (iv) nonbanks offering or providing private education loans; and (v) nonbanks offering or providing to consumers payday loans. 12 U.S.C. § 5514(a)(1).

group of entities that often lack such obligations or oversight."[13] Data aggregators hold a substantial amount of consumer financial data, and although many consumers consent to the sharing of their financial data, they are generally unaware of how that data may be used or shared. For example, a December 2021 consumer survey report on data privacy and financial app usage found that 80% of consumer respondents were largely unaware that apps use third-party providers to gather users' financial data, and only 24% knew that data aggregators can sell personal data to other parties for marketing, research, and other purposes.[14] Consumers typically do not have direct relationships with these data aggregators, and must trust that their data is handled appropriately and within the scope of their consent.

It is therefore vital for data aggregators to be supervised and examined by the Bureau to ensure that consumers' data is appropriately protected. To that end, CBA supports the U.S. Department of Treasury's recommendation that the Bureau "review its authorities to consider if and how the agency might supervise data aggregators,"[15] and specifically recommends that the Bureau affirmatively expand its supervisory authority by adding the aggregation market to the larger participant rule.[16] Absent a larger participant rule, in the context of the three-way relationship between a data provider, data aggregator, and data user, only data providers like banks would be subject to supervision and examination by the Bureau, leaving consumers uniquely vulnerable to data misuse by data aggregators and data users.

Q5. Please provide input on the approach the CFPB is considering with respect to the coverage of data providers discussed in this part III.A. What alternative approaches should the CFPB consider? For example, should the CFPB also consider covering payment account providers that are not Regulation E financial institutions as presently defined, such as providers of government benefit accounts used to distribute needs-based benefits programs? Should the CFPB consider covering any providers of credit products that are not Regulation Z credit cards? How could the CFPB clarify coverage of the proposals under consideration?

---

[13] U.S. Dep't of Treasury, *U.S. Department of the Treasury Report to the White House Competition Council - Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets* 116 (Nov. 2022), *available at* https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf.

[14] The Clearing House, 2021 Consumer Survey: Data Privacy and Financial App Usage 3 (Dec. 2021), available at https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2021-TCH-ConsumerSurveyReport_Final.

[15] U.S. Dep't of Treasury, *U.S. Department of the Treasury Report to the White House Competition Council - Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets* 117 (Nov. 2022), *available at* https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf.

16 *See, e.g.*, American Bankers Association, et al., *Petition for rulemaking defining larger participants of the aggregation services market* (Aug. 2, 2022), *available at* https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2022/08/1517000-1517653-petition-to-cfpb-for-larger-participant-rulemaking-080222.pdf.

The SBREFA outline proposes to regulate Regulation E accounts[17] and Regulation Z credit card accounts, arguing that these accounts should be regulated first "because they both implicate payments and transaction data." This approach is overly narrow and fails to capture the appropriate scope of information for enabling industry to "underwrite or help people access new products."[18] 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;
- Nonbank mortgage accounts;
- Captive auto loan accounts;[19]
- Digital wallets not otherwise an account under Regulation E;
- Cryptocurrency account;
- Alternative loans, such as buy-now-pay-later (BNPL) products;[20] 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. Director Chopra suggested, during his testimony for the Semi-Annual Report of the Consumer Financial Protection Bureau before the House Committee on Financial Services, that information captured from accounts is meant to assist industry in underwriting or helping consumers access new products.[21] If so, then it would be exceedingly misguided to limit the information industry is able to pull from data providers to only information about Regulation E accounts or Regulation Z credit card accounts. To better assess a consumer's financial health, it would be logical for industry to pull from a greater scope of financial accounts held by a consumer.

Moreover, this adjustment would reflect the reality of the market today. Millions of consumers currently share their financial data on investment and mortgage accounts with third parties,

---

[17] An "account" under Regulation E is defined as "a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes." 12 C.F.R. 1005.2(b)(1).
[18] 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)), *available at* https://www.youtube.com/watch?v=I4A09yhfmyw.
[19] As appropriately limited by Section 1029 of the Dodd-Frank Act, codified at 12 U.S.C. § 5519.
[20] It is particularly curious that BNPL products are not included in the coverage of accounts contemplated by the SBREFA Outline given the Bureau's recent focus on BNPL in other contexts.
[21] 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)), *available at* https://www.youtube.com/watch?v=I4A09yhfmyw.

which provides them with a holistic view of their finances. By excluding these account types from a Section 1033 rule's obligation to share financial data, Section 1033's intent will not be fully realized as consumers will not have full insight into control over their data nor will important consumer protections extend to data associated with those accounts.

Additionally, the Bureau's current working definition of a "data recipient" includes anyone offering (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer. This could include nonbank third parties or other banks that are not the current data providers of the consumer's information. However, there is a huge chasm in the consumer data security safeguards and protections between nonbank third parties and banks. As discussed later in this letter, banks are subject to the GLBA, Regulation P, and the Safeguards Rule,[22] as well as federal prudential regulatory oversight, whereas nonbank third parties are not. Thus, the Bureau should subject all parties in the data ecosystem to the same federal privacy and security requirements to ensure uniform consumer protection. We discuss this further in the questions related to secondary use of consumer data and data security standards.

Q6: Should the CFPB exempt certain covered data providers from any particular proposals under consideration? For which covered data providers would such exemptions be appropriate, and why? Which proposals should such data providers by exempt from, and why?

As summarized in the response to Q5, no covered data providers should be exempt from the proposals. There should be a broad scope of coverage for entities classified as data providers, banks and nonbanks alike, offering a variety of consumer financial services or products, including Regulation E accounts, Regulation Z credit card accounts, brokerage accounts, nonbank mortgage accounts, captive auto loan accounts, digital wallets, cryptocurrency accounts, alternative loans like BNPL products, and any other product or service defined as a "consumer financial product or service" under the Dodd-Frank Act. The purpose of the Section 1033 rulemaking is for consumers to have control and access to their financial information. Therefore, it is vital that data providers are not exempt from the proposals, so consumers are able to have a full understanding and control of their data.

Q12. Please provide input on the approach the CFPB is considering with respect to the authorization procedures. What alternative approaches should the CFPB consider? In providing input, please describe the authorization procedures that third parties and/or covered data providers currently employ and the benefits and drawbacks of those procedures in comparison to the procedures the CFPB is considering. What costs would third parties or covered data providers face with respect to the authorization procedures under consideration?

As described in more detail in Q13, below, CBA would strongly prefer that any authorization procedures mirror those currently used in the industry and that the authorization from the

22 16 CFR § 314

consumer for a third party to access the consumer's data come directly from the consumer, and not from the third party. CBA is concerned that the Bureau's proposed authorization procedures are contrary to current industry practice and expectations from federal banking regulators.[23] This may create additional burdens and costs on data holding institutions, reduce the benefits of data minimization, data privacy, and security for the consumer, and create unnecessary confusion.

CBA is also concerned that it is unclear in the Bureau's proposal who bears the liability and risk if a consumer's consent is obtained illegally or out of accordance with the Bureau's procedures. This furthers the argument for Bureau oversight of all parties in the ecosystem.

Q13. What alternative approaches should the CFPB consider? Please describe any additional authorization procedures or any suggested changes to the procedures the CFPB is contemplating.

Current industry practice when a consumer authorizes a third party to access their data (generally through an API) usually has two parts. First, the consumer consents directly with the data providing institution to release/provide data to the third party. Next, the data providing institution releases the data to the third party. Since data holding banks have the existing, ongoing relationship with the customer and the infrastructure to confirm the consumer's identity, it is important that the consent to share the consumer's information come directly from the consumer and not from a third party. Receiving requests to share consumer information from third parties, as opposed to consumers themselves, would create additional, unnecessary liability for data providing banks, and may create conflicts with compliance obligations under the Safeguards Rule and other data security regulatory requirements.[24] For example, it would be very difficult and costly (especially on a large scale) to determine whether consumer consent was appropriately provided to the consumer, by the third party. Under this arrangement, the data provider would have no mechanism to verify that the authorization provided by the third party reflects the consumer's legitimate understanding or that the scope of the authorization genuinely reflects the scope the consumer believes they have agreed to, potentially exposing consumers to misuse of their data.

Further, data providing banks would need to create entirely new, costly systems to authenticate third parties and determine if consumer consent authorizations are legitimate. When an API is developed, the creator configures the scope of available data that can be retrieved by authorized third parties. Under the Bureau's outline, the scope of authorization is captured by the third party, not the data provider; as a result, there could potentially be thousands of different custom permutations over what data can be accessed. A helpful analogy for thinking of APIs is to treat the data provider like a restaurant: under the SBREFA Outline, a restaurant (data provider) would need to be able to allow patrons to order any dish they want composed of any ingredient, regardless of the menu, establish a way to clarify ambiguous orders, and engage in this activity

[23] *See, e.g.*, OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" (Oct. 30, 2013); *see also* OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29" (Mar. 5, 2020).

[24] *See, e.g.*, Federal Financial Institutions Examination Council, *Authentication and Access to Financial Institution Services and Systems, available at* https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

while serving millions of patrons a day. Such a process is not technically viable and would be prohibitively costly to support. These additional costs and burdens are completely unnecessary if the consumer confirms the release of their information directly with the data providing bank, as is current industry practice.

Consumers would be better protected if they were required to provide the data provider with evidence of their authorization directly. To protect consumers, data providers should remain integral to the consumer consent process. CBA has concerns that this practice (a third party requesting consumer data) could open the door to fraud and scams, where data providing banks would have no way of confirming whether the consumer actually made the request, and scammers could create fake authorizations.

Q16. Where a covered account is held by more than one consumer, should the rule allow any consumer holding the account to authorize access, or should authorization procedures include a requirement that the third party provide authorization disclosures to and obtain consent from each consumer who is an accountholder?

As discussed in Q12 and Q13, CBA would prefer to continue using current industry practices to confirm a customer's identity and authorize the disclosure of consumer data. These practices are more secure than those proposed by the Bureau, better protect consumer data, and would not incur additional, unnecessary costs. Current industry best practices account for situations where an account is held by multiple consumers.

Q18. Should the CFPB provide model clauses and/or forms for some or all of the content of the authorization disclosure?

It would be helpful for the Bureau to provide sample forms for third parties to reference and use at their discretion to inform consumers of the third party's obligations around the collection, use, and retention of consumer data. As discussed in Q12 and Q13, CBA would prefer to continue to use current industry practices to confirm consumer identity and authorization to disclose information, as they are more secure and would not incur additional, unnecessary costs; however, CBA would support the Bureau providing a non-mandatory baseline form for authorizations that industry can flexibly modify as necessary to further enhance existing industry practices.

Q21. Please provide input on whether the full certification statement should be included in the authorization disclosure.

CBA is concerned that the Certification Statement described in the outline of proposals appears as though it is intended to create a liability framework between consumers and third parties but does not appear to discuss liability for noncompliance with a potential Section 1033 rule.

Q22. Please provide input on the approach the CFPB is considering with respect to these categories of information. What alternative approaches should the CFPB consider? In part III.C.1.vi, the CFPB is seeking feedback on what other categories and data elements not identified in the subsections below should be covered.

CBA has several concerns regarding the six categories[25] of information the Bureau has proposed in the outline.

Non-tokenized account information
CBA has concerns that certain less secure consumer information such as account numbers and routing information would be required to be disclosed to authorized third parties under the Bureau's proposal, rather than more secure tokenized account information, which is the current industry best practice. 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.[26] 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.[27]

Information on transactions that have not yet settled
There is significant risk to consumers in sharing information with authorized third parties that is likely to change, such as automatic online banking transactions that have been set up, but have not yet occurred, or a hold placed on a debit or credit card that is different from the final charged amount. Due to the fact that, by definition, these amounts are subject to change, they give consumers and authorized third parties an inaccurate view of the consumer's data. Moreover, data providers have different practices that could distort information provided to an authorized third party. For example, one data provider may have a different practice of handling and recording pending charges than another data provider, which could result in confusion for third parties pulling this information and distort the overall picture of a consumer's financial health. If data providers are obligated to share this information with authorized third parties, then liability for any consumer harm resulting from sharing this information should rest with the data recipient that requested this data.

Back-end processing information
The Bureau should not require that data providers share information about prior transactions not typically shown on periodic statements or portals, such as back-end processing or routing information. Sharing such information would place a significant financial burden on data

[25] The SBREFA Outline identifies six potential categories of information: (i) periodic statement information for settled transactions and deposits; (ii) information regarding prior transactions and deposits that have not yet settled; (iii) other information about prior transactions not typically shown on periodic statements or portals; (iv) online banking transactions that the consumer has set up but that have not yet occurred, (v) account identify information; and (vi) other information.
[26] For example, The Clearing House has launched Secure Token Exchange (STE) for payments on the RTP network to tokenize account numbers in a way that does not later existing payment authorizations. More information about STE is available here: https://www.theclearinghouse.org/payment-systems/secure-token-exchange.
[27] While Federal consumer financial laws often protect consumers from loss in cases of unauthorized transfers, the time and effort required to initiate claims after the fact also creates a negative consumer experience.

providers, as they would need to build entirely new systems for sharing information that they do not currently share. Moreover, it is not clear how this information would benefit consumers, since information about the parties involved in processing an ACH debit does not appear related to underwriting or facilitating consumer access to new financial products and services. Further, the disclosure of this information could overwhelm or confuse consumers. Additionally, requiring data providers to release this additional information that is above and far beyond what current online banking profiles and APIs cover would result in substantial costs.

Account identity information and potential fraud

The SBREFA outline lists an expansive list of fifteen pieces of information[28] about a consumer that a bank would need to make available to a consumer and to an authorized third party as "account identity information." It is unclear why some of the data elements included are necessary to facilitate underwriting or consumer access to new products. Several of the proposed data elements, such as citizenship or immigration status and veteran status, are unrelated to transactions themselves or are not regularly collected. There is significant risk that such information - if misused by a third party or if accessed by fraudsters through a data breach - could be used to perpetuate fraud and harm consumers. Additionally, requiring data providers to release this additional information that is above and far beyond what current online banking profiles and APIs cover would result in substantial costs and take a significant amount of time to implement.

Costly other information that has no benefit to consumers

The final category of information, titled simply "other information,"[29] is overly broad and not particularly relevant to a consumer's access to their own information. This list of "other information" is far too expansive, and the Bureau has not sufficiently articulated what the benefit of consumers and authorized third parties accessing this information would be. The disclosure of such information to nonbank third parties could place financial institutions at a competitive disadvantage with competitors that may not be subject to the same regulatory framework nor be required to share similar information with financial institutions in return. This tension further highlights the need to define the scope of "covered persons" broadly. Requirements regarding the disclosure to consumers of the types of information discussed in the Bureau's outline are already addressed in other regulations. For example, the Fair Credit Reporting Act (FCRA) and Regulation B that requires lenders to, among other things, notify consumers when their credit report is pulled, provide adverse action notices, inform consumers of the ability to obtain free credit reports, so it is unclear what the consumer benefit would be in mandating data providers to share consumer reports from consumer reporting agencies with authorized third parties. Moreover, data providers' agreements with credit reporting agencies typically prohibit data providers from sharing credit report information. Additionally, there does not appear to be any

[28] The fifteen pieces of "account identity information" include: (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.

[29] The category of "other information" includes: (i) consumer reports from consumer reporting agencies, such as credit bureaus, obtained and used by the covered data provider in deciding whether to provide an account or other financial product or service to a consumer; (ii) fees that the covered data provider assesses in connection with its covered accounts; (iii) bonuses, rewards, discounts, or other incentives that the covered data provider issues to consumers; and (iv) information about security breaches that exposed a consumer's identity or financial information.

consumer benefit associated with requiring banks to share information with authorized third parties about banks' security breaches, particularly due to the fact banks are already required to notify consumers of security breaches. Requiring data providers to release this additional information that is above and far beyond what current online banking profiles and APIs cover would result in substantial costs.

In addition, although not explicitly discussed in the SBREFA Outline, to the extent the Bureau contemplates specific account numbers (either for accounts as defined under Regulation E or for credit card accounts under Regulation Z) being transferred, in full, between financial institutions so that from the consumer's perspective, the account number does not change, there are serious and significant network and system challenges. There are also risks for widespread fraud and safety and soundness concerns that must be fully considered and addressed across the industry.[30] The costs and implementation time period to introduce such ability is likely to be extremely significant for financial institutions regardless of its size.

Q23. Is additional clarity needed with respect to the data elements the CFPB is considering proposing? What further information would be helpful? For example, should the rule set forth all the specific data elements that the rule requires covered data providers to make available?

As noted in the response to Q22, CBA urges the Bureau to more closely consider the general industry shift toward tokenization in a final Section 1033 rule. Specifically, data providers should have the option to share a tokenized deposit account and routing number in lieu of the actual deposit account number to authorized third parties. Any requirement that forces banks to share actual deposit account numbers introduces unnecessary risk into the payments ecosystem, as third parties, or any other entities that gain access to actual deposit account numbers and routing numbers, could initiate fraudulent transactions or engage in other criminal activity. The Bureau should also consider how it can support standardized data definitions and maintain alignment of data definitions with existing regulatory definitions to reduce implementation frictions and costs and to better facilitate the delivery of the data the consumer intends to share.

Q26. Please provide input about the data security and privacy risks that would result from a requirement that covered data providers make available to authorized third parties the above-described information.

As noted in the response to Q22, the fifteen pieces of information that would be made available to a consumer and to an authorized third party as "account identity information" is stunningly expansive and results in a significant portfolio on the consumer, not just on the consumer's financial data, placing consumers at increased risk should the data be misused. Mandating third party access to certain sensitive identity data, such as a consumer's Social Security number or demographic information, raises serious privacy and operational concerns.

[30] *See generally* Director Chopra's Prepared Remarks at Money 20/20 (Oct. 25, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/.

The SBREFA Outline does not include accreditation standards that authorized third parties would need to meet; even though a third party may be authorized by a consumer to access that consumer's financial information, banks may have third-party risk management guidance obligations or other best practices that would prevent the bank from sharing this information with the third party, particularly when the bank itself has not reviewed and approved of the third party.

CBA would support reframing a potential rule to have third parties request certain sensitive information directly from the consumer, such as race, ethnicity, or a Social Security number. Indeed, there may be merit in having a healthy degree of friction for consumers when it comes to intentionally deciding to share this sensitive information with a third party. Allowing third parties to access this account identity information could result in circumstances where a consumer quickly clicks through an agreement with a third party and is unaware that they have authorized the third party to access highly sensitive data elements about them. A better approach to mitigate this risk would be for the Bureau to distinguish between information that consumers can access about themselves, and information that an authorized third party can access from a data provider about that consumer; it is only logical that a consumer should have more access to their own information than a third party should, and if the consumer truly wants to provide the third party with this sensitive identity data, they can do so accurately and directly.

Q27. Please provide input on whether the above-described confirm/deny approach would be feasible to implement and could suffice to achieve the contemplated consumer benefits of authorized third-party access to consumer financial data. Are there alternative approaches that the CFPB should consider?

The validity of a confirm/deny approach - which, as described by the SBREFA outline, would require the authorized third party to present a data provider the identity information that the consumer provided to the authorized third party, after which the data provider would confirm or deny that the information presented is the information that the data provider has on file - would necessarily depend on the security and robustness of the data ecosystem.

As summarized in Q26, there is significant risk associated with enabling authorized third parties to access consumers' sensitive identity data, such as Social Security numbers and demographic information. There are numerous issues that would need to be addressed in the confirm/deny approach. Significantly, the number of queries that an authorized third party can send to the data provider would need to be limited; otherwise, a malicious authorized third party could theoretically query the data provider enough times until they correctly guess the consumer's sensitive identity data. Based on the richness of this sensitive identity data, authorized third parties could use this unlimited confirm/deny approach to easily initiate synthetic identity fraud. For any confirm/deny approach to work appropriately, data providers will need to have the ability to independently verify the third party and be able to decline queries from third parties the data provider deems suspicious.

The technological and operational cost of a confirm/deny approach would likely make the entire effort infeasible. The tools necessary for maintaining APIs that confirm/deny user-submitted

identity information would be highly complex and hard to operationalize in practice. Such systems would need to rely on numerous types of matching logics to handle different queries for the same set of information in the data provider's possession; for example, an API that confirms/denies identity information would need to determine whether "Joe Smith," "Joseph Smith," and "J. Smith" all refer to the same identity in order to accurately confirm/deny. The apparent consumer benefit does not outweigh these significant costs, particularly when the consumer could provide this information to a third party themselves.

Q28. Please provide input on whether the CFPB should require a covered data provider to make available to a consumer or an authorized third party any category of information other than the five categories of information discussed in part III.C.1 above. Are there any other data elements not described herein that the CFPB should consider proposing?

The Bureau should not consider proposing additional data elements beyond the six categories already outlined in the SBREFA outline. Moreover, as summarized in Q22 and Q26, even those six categories are overly broad and should be scaled back.

Q29. What would be the potential costs or challenges of requiring the disclosure of some or all the information outlined in this part III.C.1.vi? How could the CFPB reduce costs and facilitate compliance for small entities?

As summarized in Q22, the proposed list of "other information" is far too expansive and the Bureau has not sufficiently articulated what the benefit of consumers and third parties accessing this information would be. For example, no new consumer benefits are created by requiring banks to share information with authorized third parties about banks' security breaches, particularly due to the fact banks are already required to notify consumers of security breaches. Requiring banks to develop and maintain entirely new systems to provide information that banks already provide to consumers in compliance with other laws and regulations would impose unnecessary costs on banks.

As a threshold matter, providing information about security breaches appears inconsistent with the plain language and intent of Section 1033, which requires covered persons to make available information in the control or possession of the covered person "concerning the consumer financial product or service that the consumer obtained from such covered person," including information related to any transaction, series of transactions, or account information including costs, charges, and usage data.[31] Information about security breaches goes well beyond the information that is contemplated by the statute, does not concern the offering of the product or service, would not relate to account or transactional information, and would not be readily available by the data provider.

[31] 12 U.S.C. § 5533(a).

Second, the proposed requirement to provide information to consumers about security breaches that exposed a consumer's identity is potentially duplicative and unnecessary for financial institutions. If this requirement remains in the final rule, an exemption for financial institutions is recommended, as well as a requirement that authorized third parties also be required to provide the same level of information related to security breaches as financial institutions to both regulators and consumers. Currently, financial institutions are already required to notify customers, when their personally identifiable information is affected in a security incident under both federal (GLBA, the federal banking agencies' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information,[32] and the recently enacted joint agency computer security incident notification rule[33]) and applicable state law. It is unclear from the SBREFA Outline how additional requests for information related to security breaches would impact existing laws. Regardless of its impact, it appears, at best, to be a duplicative requirement for information already directly held by the consumer. Allowing requests for information related to historical security breaches will add additional costs to data providers without providing any new information or benefit to consumers. Moreover, based on the stated goals of the proposal, there would be no purpose or benefit to consumers in allowing a third party to request information or obtain information about security breaches that occurred at the data provider and may have affected the consumer in the past. The consumer's data is already in the possession of the data provider, and the consumer is now seeking to provide access to an additional third-party.

Third, by allowing authorized third parties to make requests for information related to consumers for prior security breaches, the chances that impacted consumers are subsequently harmed (or harmed again), either through account freezes or temporarily being unable to access certain funds, only increases as specific information about consumers and their previously compromised accounts could potentially be widely circulated.

More broadly than the category of "other information," several of the proposals related to information a data provider would be required to disclose to a consumer or authorized third party would be exceedingly costly to implement. Many of these net new requirements would require data providers to develop and maintain entirely new systems and procedures. For example, the SBREFA Outline states that data providers would need to make available information with respect to settled transactions and deposits that generally appear on the periodic statements provided for asset accounts and for credit card accounts. These periodic statements are governed by the form and disclosure requirements found in Regulation E and Regulation Z, which are heavily detailed and specific. Under this requirement in the SBREFA Outline, data providers would need to develop an entirely new method of displaying this information to the consumers in a manner that complies with the form and disclosure requirements in Regulation E and Regulation Z, which include formatting requirements for physical presentation of this information that does not easily translate to digital presentations of the same information. Data

[32] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005).
[33] Computer-Security Incident Notification Requirements for Banking Organizations and Their banking Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021).

providers would be able to share this information in a more cost-effective manner if the Bureau were to amend the required form and disclosure requirements for periodic statements under Regulation E and Regulation Z, and modernize those form and disclosure requirements for digital means to ensure that the disclosure requirements can be easily translated to a digital access portal or API.

The Bureau also significantly overestimates the degree to which banks have already implemented APIs and the cost that would be associated with undertaking such an endeavor. Not all of CBA's member institutions currently have APIs that could provide the information outlined in the SBREFA Outline to authorized third parties and it would take a significant amount of time and resources to develop such APIs. CBA's member institutions report that entering into a strategic partnership to set up an API is a significant cost and that API can take well over twelve months to develop. Additionally, the Bureau contemplates consumers accessing the information outlined in the SBREFA Outline through a data access portal, which will require data providers to spend a significant amount of time and resources on technology investments to create and build out these portals.

Q32. How should the CFPB interpret "confidential commercial information"? What existing legal standards, if any, should inform the CFPB's considerations regarding interpreting that term in the context of Dodd-Frank Act section 1033? To what extent should a covered data provider's ownership interest in such information be a factor?

CBA generally supports the Bureau including an exception for "confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors." However, there is significant risk that if data providers are required to make the underlying data for those algorithms or predictors to authorized third parties, those third parties can ultimately reverse engineer the proprietary information and algorithms, effectively undermining the exception for confidential commercial information. Congress clearly intended to create an exception for confidential commercial information, and to preserve the integrity of this exception, data providers should be able to place appropriate controls on the authorized third parties receiving the elements of that confidential commercial information to prohibit reverse engineering. Further, to ensure that third parties do not attempt to reverse engineer confidential commercial information from the data elements they do receive from data providers, it is imperative that there be an enforcement mechanism, in addition to litigation, for data providers to protect themselves. For example, data providers could be permitted to cut off access of third parties if a data provider believes a third party is reverse engineering confidential commercial information, or authorized third parties could be required to demonstrate that they have not used information obtained from a data provider to reverse engineer the data provider's confidential commercial information. The Bureau should explicitly prohibit this type of anticompetitive behavior in a final rule.

Q40. Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers

through an online financial account management portal and to give consumers the option to export the information in both human and machine readable file formats. What alternatives should the CFPB consider?

The proposal to make information available directly to consumers, if a data provider has enough information to reasonably authenticate the consumer's identity and reasonably identify the information requested, would require extensive new, and costly functionality into existing online banking consumer-facing platforms. The Bureau also underestimates the cost of requiring data providers to provide account-related information via online human-readable formats, online machine-readable formats, and via a third-party accessible API, particularly because very few data providers would have all these capabilities built out already. This requirement would result in a significant drain on data providers' resources and impose a sizable financial cost. CBA urges the Bureau to consider either fewer requirements (either human or machine readable, for example).

Q41. Do covered data providers currently charge consumers specific fees (i.e., fees other than periodic account maintenance fees) to access information through an online financial account management portal or to export information in a human or machine readable format? What would be the impact on covered data providers and consumers if covered data providers were restricted from charging specific fees?

The Bureau must clarify the scope of entities that fall within the definition of "consumer." The SBREFA Outline summarizes that the Dodd-Frank Act defines the term "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual."[34] Based on this definition, an authorized third-party could fall within the meaning of the term "consumer." This is astoundingly problematic, particularly because data providers will need to be able to charge reasonable fees to third parties accessing consumer information through a third-party data access portal to offset the necessary infrastructure developments to handle the increased strain that will be placed on data providers' systems. The Bureau must clarify that a "consumer", for purposes of a Section 1033 rulemaking, refers to the individual account holder with whom the data provider has a relationship, and does not encompass agents or representatives like authorized third parties.

While many CBA members do not currently charge consumers specific fees to access information through their existing customer-facing online financial account management portals, the SBREFA Outline contains extensive new requirements for account management portals that may require data providers to charge for the costly build-out of new technology. Some CBA members currently charge data recipients fees associated with the reasonable costs associated with providing the requested data and should continue to be allowed to do so, consistent with their existing contractional agreements.

Q42. If there are data elements that covered data providers are not currently making available to a consumer in electronic form through online financial account management

[34] 12 U.S.C. § 5481(4).

portals, please describe any considerations that would weigh against requiring covered data providers to make such data elements available through such portals. For example, are certain types of information the CFPB is considering typically retained in records that are not easily made available in electronic form, such as paper or audio recordings? Are there any other considerations that impact the costs of requiring covered data providers to make such information available in electronic form through online financial account management portals?

As noted in the response to Q40, the information that would be shared by data providers with consumers through a direct access portal would include information that is not currently shared with consumers through such portals. For example, payment routing information is not typically displayed to the consumer, and data providers would need to implement entirely new functionality to share information like this through a direct access portal. It is not clear how allowing consumers to access this information would benefit them or the market. Sharing this information would impose a substantial financial and resource burden on data providers, as they would need to build out entirely new capabilities in their data access portals to identify and share this information with consumers. This type of data may also increase the risk to the safety and security of the consumers' accounts and increase fraud within the ecosystem, leading to a worse consumer experience.

Q44. Do covered data providers have policies and procedures in place to ensure that the information currently made available through online financial account management portals is not made inaccurate due to the way the portal operates or the way the information is transmitted to the consumer? If so, please describe these policies and procedures.

Section 1033 of the Dodd-Frank Act requires data providers to make available to consumers information in the data provider's control or possession concerning the consumer financial product or service that the consumer obtains from the provider. Section 1033 of the Dodd-Frank Act does *not* create new obligations for data providers regarding data accuracy. As such, a potential Section 1033 implementing rule cannot, and should not seek to impose new data accuracy obligations on data providers.

Through the ordinary course of doing business, data providers already perform assessments to validate, or to correct, information in data providers' control. Data providers do not knowingly provide inaccurate information, nor do they have an interest in doing so, and they are prohibited from doing so by several existing federal and state laws. In fact, data providers are obliged to correct inaccurate information as soon as they determine its inaccuracy. A Section 1033 rulemaking should not add new obligations related to data accuracy, as they are not contemplated by the statutory text and many data providers already comply with robust data accuracy requirements. Layering additional, and potentially conflicting obligations would create confusion and costs for data providers and would not provide any additional benefit to consumers.

Q50. Please provide input on the approach the CFPB is considering with respect to the third-party access portal proposal. What alternative approaches should the CFPB consider?

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 in the SBREFA Outline. If the SBREFA Outline's proposals were implemented as currently drafted, data providers would need to account for the expansion of mandatory data elements, changes in how authorization is collected, requirements to expand frequency of access and/or channel uptime, the potential absence of reasonable time/place/manner restrictions by data providers, the significant expansion in risks posed to consumer data and associated safety and soundness concerns, and an increase in the number of third parties each data provider would be required to engage with directly. Each of these changes in isolation would impose significant costs on data providers that already utilize APIs; these potential changes in the aggregate would impose overwhelming costs.

If a data provider is required to offer access to a third party through an API, then the data provider should be permitted to block all screen scraping by third parties. Screen 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 providers to effectively block screen scraping and push usage of safer APIs. It is challenging and costly for data providers to effectively prevent screen scraping and to ensure only consumer-authorized data is shared. Many data providers are unlikely to have the capacity to know when, and in what volume, a third party engages in screen scraping. Even for larger data providers, it is expensive to differentiate and block automated web scraping while not inadvertently blocking real consumer traffic; distinguishing the two has only become more difficult as third parties now repeatedly modify their automated scripts to appear more human and bypass efforts to restrict screen scraping.

Q52. With respect to covered data providers that have not yet established a third-party access portal at the time the rule is final and effective, should the CFPB require that they make information available to authorized third parties before they establish a third-party access portal? Would such a requirement necessitate covered data providers allowing authorized third parties to engage in screen scraping? Are there alternatives to screen scraping that a covered data provider could implement to make information available to authorized third parties in electronic form while establishing a third-party access portal?

Even if a third-party access portal is not yet established at the time a section 1033 rule is finalized, screen scraping should not be permitted as an alternative. As discussed in the response to Q50, if data providers are required to offer access to an authorized third party through a third-party access portal, the data provider should be permitted to block all screen scraping by third parties. Screen scraping is a fundamentally unsafe method of access. Making information

available to a third party through screen scraping rather than a third-party access portal wholly undermines attempts to empower consumers to define the scope of their data that a third party can access. Further, screen scraping may cause consumer harm. If screen scraping is permitted as an alternative to API access, any tailoring of the consumer's authorization vanishes and a third party could have access to consumer information beyond what the consumer has authorized.

Q55. Should covered data providers be required to permit screen scraping when the covered data provider's third-party access portal experiences a service interruption? What records could demonstrate that a service interruption to a third-party access portal has occurred? What alternatives to screen scraping should the CFPB consider to reduce interruptions to authorized third party information access when a third-party access portal experiences a service interruption?

The Bureau should not permit screen scraping when a data provider's third-party access portal experiences a service interruption. As a threshold matter, it is exceedingly unlikely that a data provider's third-party access portal would experience any extended service interruptions while the data provider's website would still be functioning such that a third party could screen scrape from it.

As summarized in Q50, screen scraping is an unsafe method of access and the Bureau should move to sunset the practice. Assuming that a data provider's website would even be functional while an API is experiencing a service interruption, allowing third parties to engage in screen scraping during periods of API service interruptions poses significant harm and undermines consumer protection. Permitting screen scraping in these instances could result in volatility in the traffic a data provider's website experiences, which itself could lead to service interruptions for that website and halt both consumer and third-party traffic to the website.

Further, as discussed in Q52, screen scraping may cause consumer harm. If screen scraping is permitted during a service interruption, there is risk that a data provider would be unable to honor a consumer's authorization in such an instance. For example, if a consumer has permissioned an authorized third party access to a narrow set of data via a data provider's API, the only way to honor that consumer-authorized narrow scope of information would be through an API; if a third party were also able to screen scrape the information, the third party would have access to data beyond the consumer's narrow authorization, including potentially related to products and services that currently fall beyond accounts under Regulation E and Regulation Z. Further, allowing screen scraping as a backup in instances of third-party access portal service interruptions is likely to confuse consumers, and lead to potential data security issues, as consumers would be required to both authenticate with their data provider to enable the third party's API access and then separately share their access credentials with the third party.

Q56. To the extent screen scraping is a method by which covered data providers are permitted to satisfy their obligations to make information available, how could the CFPB mitigate the consumer risks associated with screen scraping? For example, should the CFPB require covered data providers to provide access tokens to authorized third parties to use to screen scrape so that third parties would not need a consumer's credentials to access the online financial account management portal? Alternatively, should authorized

third parties be restricted from retaining consumer credentials indefinitely? For how long do authorized third parties need to retain consumer credentials? If the answer depends on the use case, please explain.

As summarized in Q50, screen scraping is an unsafe method of access and the Bureau should move to sunset the practice. Although the use of access tokens for screen scraping is a preferred alternative to screen scraping using a consumer's credentials and may alleviate some financial burden as an alternative for institutions transitioning to an API, the Bureau should not mandate that data providers provide access tokens to authorized third parties for screen scraping. APIs allow data providers to enable third party data access that matches the scope, duration, and frequency that has been authorized by the consumer for the third party. Using a token to screen scrape allows for none of those limitations that match consumer authorization; even though such a method would better protect a consumer's access credentials, it does nothing to actually protect the scope of the consumer's authorization of the third party's access.

Q57. Please provide input on whether CFPB-defined standards are needed to promote the availability of data to authorized third parties, whether certain aspects of the regulation of third-party access portals are better suited to be regulated by industry participants, and how the CFPB can promote the development of industry standards. How should the CFPB take account of the voluntary standards and guidelines that some industry participants have developed as the CFPB is considering regulating third-party access portals?

The financial services industry, through industry standard-setting bodies, should continue to take the lead in developing the standards for consumer-authorized data access. As CBA summarized in its comment on the Bureau's Advanced Notice of Proposed Rulemaking (ANPR) for Section 1033, "[p]rescriptive standards would impede industry flexibility to adapt to changes in technology. A Bureau led effort would likely include lag time between the emergence of new threats or opportunities and any regulatory response." [35] Instead, industry standard-setting bodies are better suited to respond to the quickly evolving technological landscape. For example, FDX - a consortium of data providers, data aggregators, data recipients, and other key industry participants[36] - has developed a common, interoperable, and royalty-free technical standard for user-permissioned financial data sharing.[37] Other industry-setting standards include: The Clearing House's Connected Banking Initiative, which advocates for new technology standards and infrastructure, risk management requirements and legal agreements, and ongoing industry collaboration;[38] Akoya, which provides consumers with more control and security when connecting their bank accounts to third parties;[39] and Afinis, which furthers the work of Nacha's Payments Innovation Alliance API Standardization Industry Group to advance standardization

[35] CBA, *Letter to Consumer Financial Protection Bureau re: Docket No. CFPB-2020-0034 / RIN 3170-AA78 Consumer Access to Financial Records* (Feb. 4, 2021), *available at* https://www.consumerbankers.com/sites/default/files/CBA%20Sec%201033%20ANPR%20Comment%20FINAL%2002042021.pdf.
[36] FDX, *Members*, *available at* https://financialdataexchange.org/FDX/FDX/The-Consortium/Members.aspx?hkey=362ecd23-b752-48aa-b104-a99e916276c8.
[37] FDX, *About FDC - Our Mission*, *available at* https://financialdataexchange.org/FDX/FDX/About/About-FDX.aspx?hkey=dffb9a93-fc7d-4f65-840c-f2cfbe7fe8a6.
[38] *See* The Clearing House, *Connected Banking*, *available at* https://www.theclearinghouse.org/connected-banking.
[39] *See* Akoya, *Customers*, *available at* https://akoya.com/products/customers.

efforts across the financial services ecosystem through formal governance.[40] Moving away from these frameworks and instead granting the Bureau the primary role in defining standards will hamper innovation and likely result in standards that are impractical to implement or lock the industry into legacy technologies and standards that fail to address needs in the evolving market.

Q59. Please provide input on the third-party portal availability factors under consideration. Are there any other factors or alternative approaches the CFPB should consider?

In the SBREFA Outline, the Bureau contemplates five categories of factors to determine whether a data provider has satisfied its obligation to provide a third-party access portal.[41] As a general matter, these five factors functionally serve as service level agreements (SLAs) on data providers. Data providers would face significant costs in measuring and demonstrating compliance with these requirements, and as such may need to charge reasonable fees to build out the necessary infrastructure to comply with reasonable SLAs.

The Bureau has failed to evaluate the practical realities of making a third-party portal available and the necessary tradeoffs between these factors. Permitting an increasing number of third parties to access a data provider's API will introduce additional costs on data providers as they attempt to support the higher volumes of traffic to the APIs. Even with an investment in additional resources to support a higher volume of traffic to an API, there is a very real risk that the cumulative volume of third-party traffic can endanger a data provider's systems and impact uptime and latency. To address this risk, data providers should be able to maintain the ability to implement reasonable time, place, and manner restrictions, including reasonable throttling of access by third parties to the API to protect the infrastructure and to help ensure direct consumer access when needed, which implicates the access caps factor. The SBREFA Outline does not appear to acknowledge the reality that planned service outages, a decrease in latency, or the presence of reasonable access caps may be necessary to facilitate API access overall and prevent outages and errors across the entire system.

Moreover, the Bureau's factors should acknowledge many of the technological realities in the marketplace today. For example, a large share of data aggregation use cases can be supported by a single data pull by a third party per day, yet it would appear that a data provider would be penalized for imposing an access cap if the data provider configured their third-party access portal to reflect this reality; as a result, data providers could be saddled with the unreasonable burden of facilitating multiple data pulls per day even though this rarely occurs in the market and risks overwhelming their technology systems, which could result in unplanned outages.

Q60. Should the CFPB articulate similar availability factors with respect to the online management account portal proposal described above in part III.D.1?

---

[40] *See* Afinis, *Afinis Interoperability Standards*, *available at* https://www.nacha.org/afinis-interoperability-standards?_ga=2.210268821.1693382936.1672853523-1994227330.1672853523&__hstc=192855669.4f7783fe3cf94d74b69a3e05783aa02f.1672853523530.1672853523530.1672853523530.1&__hssc=192855669.1.1672853523530&__hsfp=1383244671.

[41] The third-party portal availability factors under consideration in the SBREFA Outline are: (i) uptime; (ii) latency; (iii) response to planned and unplanned outages; (iv) error response; and (v) access caps.

As noted in the response to Q59, these factors operate functionally as SLAs which data providers would need to spend a significant amount of time and resources on to measure and demonstrate compliance with. Imposing a similar set of availability factors on the online management account portal in addition to the third-party access portal would double that burden.

If the Bureau were to impose these factors on both the online management account portal for consumers and the third-party access portal, it is incumbent upon the Bureau to ensure the standards data providers must meet for the third-party access portal are not greater than the standards data providers must meet for the online management account portal for consumers. The data provider has the primary relationship with the consumer, not with the authorized third party; as such, it is only right that the more rigorous standards apply to the first-party digital channel rather than the third-party access portal where the consumer is not necessarily present in the flow of data.

Q61. Please provide input on specific elements or standards that might be considered under these forms of regulation. For example, are there circumstances in which it would be appropriate for a performance standard to require 100 percent availability? What kind of policies and procedures would reasonably be required to ensure availability of information to authorized third parties?

As discussed in the response to Q59, the SBREFA Outline does not adequately contemplate the practical realities of making a third-party access portal available and the necessary tradeoffs between these factors. There is a very real risk that the cumulative volume of third-party traffic will negatively impact the uptime and latency factors of a data provider's third-party access portal. Data providers, seeking to improve their systems' uptime and latency factors may need to take action that would implicate the access caps factor. As a result, it is unrealistic for the Bureau to require data providers' systems, or any systems, to meet 100% availability for one performance standard, let alone multiple performance standards.

Q63. What would be the impact on covered data providers, authorized third parties, and consumers if covered data providers were or were not restricted from charging specific fees under the rule in order to access information through a third-party access portal?

There is value in covered data providers being able to charge reasonable fees to authorized third parties that are accessing information through a third-party access portal due to the strain this access will place on data providers' systems. As discussed in the response to Q59, the five factors listed in the SBREFA Outline functionally serve as SLAs that a data provider would need to ensure that their third-party access portal meets. Building out the functionality to meet these SLAs and handle the significant uptick in third-party traffic would impose a significant financial burden on data providers regardless of size. To offset this new, exorbitant cost, data providers should be allowed to charge fees to build out and maintain the necessary infrastructure to comply with reasonable SLAs. Further, reasonable fees will help ensure that only the data that is needed to provide the consumer the requested product or service is accessed, as additional or more frequent requests would be more expensive. Absent the ability to charge fees, many data

providers simply may not be able to afford to develop a third-party access portal that meets standards required by the Bureau.

Q66. Please provide input on the approach the CFPB is considering with respect to ensuring that covered data providers transmit consumer information accurately. What alternative approaches should the CFPB consider?

As discussed in the response to Q44, Section 1033 of the Dodd-Frank Act does not impose new obligations on data providers regarding data accuracy, and as such, a Section 1033 rulemaking should not go beyond the statutory text to create new data accuracy obligations for data providers. Data providers already perform assessments to validate, and to correct, information in their control to avoid providing inaccurate information.

Q72. Please provide input on what steps the CFPB should take to prevent third parties that do not satisfy the conditions described above from obtaining information. Are there other conditions beyond what is described here that a third party should need to satisfy before a covered data provider is obligated to make information available? Are there circumstances in which third parties should be permitted to access information even if they do not satisfy the conditions the CFPB is considering proposing?

When evaluating how to prevent third parties that either (i) do not have evidence of their authority to access information on behalf of a consumer, (ii) information sufficient to identify the scope of the information requested, and/or (iii) information sufficient to authenticate the third party's identity from accessing consumer information, the Bureau should consider how data providers would even be able to verify a third party's identity. Outside of bilateral contracts between data providers and third parties or an industry registry of authorized third parties, it is going to be difficult for data providers to reasonably operationalize the requirements to directly verify the identity of the potentially thousands of third parties or ensure downstream data security measures. Today, data providers typically verify the completeness of third-party authorizations through contractual obligations between data providers, data aggregators, and data recipients.

The Bureau should permit data providers to verify that third parties are in compliance with certain minimum requirements, including the Safeguards Rule and Safeguards Guidelines under the GLBA, as further discussed in the responses to Q111 and Q112. Data providers should be able to restrict access by third parties that data providers reasonably believe do not meet those minimum requirements.

Additionally, given the fact that downstream misuses of consumer information occur outside the confines of a data provider's system, data providers should be indemnified by the third parties for any costs or losses that the data provider may incur from actions attributable to the third party's access to the consumer's information. CBA also recommends that the Bureau coordinate with the prudential regulators to ensure consistency in requirements for participants throughout the data access ecosystem, especially with respect to third-party activities and consumer protection.

Q73. Please provide input on the approach the CFPB is considering. What alternative approaches should the CFPB consider? Should covered data providers be able to obtain evidence of authorization directly from a consumer, rather than through an authorized third party? Is there additional information, besides the above-described evidence, that a covered data provider should receive before a third party should be treated as authorized to access the consumer's information?

As discussed in Q12, Q13, Q14, and Q16, CBA urges the Bureau to mirror the authorization procedures currently used in the industry and that the authorization from the consumer for a third party to access the consumer's data come directly from the consumer, and not from the third party. CBA is concerned that the Bureau's proposed authorization procedures are contrary to current industry practice. This may create additional burdens and costs on data holding institutions, as well as unnecessary confusion and risk that the consumer's authorization is not accurately conveyed to the data provider.

As stated in response to Q13, current industry practice when a consumer authorizes a third party to access their data (generally through an API) generally has two parts. First, the consumer consents directly with the data providing institution to release/provide data to the third party. Next, the data providing institution releases the data to the third party. Since data holding banks have the existing, ongoing relationship with the customer and the infrastructure to confirm the consumer's identity, it is important that the consent to share the consumer's information come directly from the consumer and not from a third party. Receiving requests to share consumer information from third parties, as opposed to consumers themselves, would create additional, unnecessary liability for data holding banks, and may create conflicts with compliance obligations under the Safeguards Rule and other data security regulatory requirements.[42] For example, it would be very difficult and costly (especially on a large scale) to determine whether consumer consent was provided to the consumer, by the third party, appropriately. Under this arrangement, the data provider would have no mechanism to verify that the authorization provided by the third party reflects the consumer's legitimate understanding or that the scope of the authorization genuinely reflects the scope the consumer believes they have agreed to.

Further, data holding banks would need to create entirely new, costly systems to authenticate third parties and determine if consumer consent authorizations are legitimate. When an API is developed, the creator configures the scope of available data that can be retrieved by authorized third parties. Under this proposal, the scope of authorization is captured by the third party, not the data provider; as a result, there could potentially be thousands of different custom permutations over what data can be accessed.

Consumers would be better protected if they were required to provide the data provider with evidence of their authorization, and the scope of that authorization, directly. CBA has concerns that this practice (a third party requesting consumer data) could open the door to fraud and scams, where data providing banks would have no way of confirming whether the consumer actually made the request, and scammers could create fake authorizations. This concern is

[42] *See, e.g.*, Federal Financial Institutions Examination Council, *Authentication and Access to Financial Institution Services and Systems, available at* https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

particularly acute if there is no control on the size of the third part or independent verification of the compliance infrastructure of a given data recipient.

Q74. Please provide input on what type of evidence of revocation of a third party's authorization a covered data provider should be required to receive before they terminate access.

As noted in the response to Q73, authorization should be obtained directly from the consumer, rather than from the third party. The converse should also be true, and consumers should affirmatively inform data providers when they wish to revoke a third party's access to the consumer's information to ensure consumers' data is only shared to the extent authorized by the consumer.

Q75. To reduce the risk of potentially fraudulently obtained authorizations, should a covered data provider be required to notify a consumer of a third party's initial access attempt (such as by providing consumers a copy of the evidence of authorization submitted by a third party), or be permitted to confirm with the consumer the authorization of a particular third party before making information available? To enable consumers to monitor third-party access to their account information, should covered data providers be required to inform consumers of which third parties are accessing information pursuant to a purported authorization?

As discussed in Q73, data providers should obtain authorization directly from the consumer, rather than from the third party. As noted in the response to Q73, a data provider contacting a consumer about a third party's initial access attempt may confuse consumers and cause them to mistakenly authorize access for third parties because the request is coming from the data provider the consumer is familiar with rather than from the third party. It is appropriate that evidence of authorization be given to the data provider by the consumer, rather than by the third party. This would signal to data providers that the consumer understands and consents to the scope of authorization they have agreed to with the third party based in their distinct contractual agreement. This would also eliminate the need for consumers to be informed of which third parties are accessing information pursuant to authorization because the consumer would have affirmatively informed the data provider which third parties the consumer has granted access to their information. Finally, it would reduce consumer confusion as the data provider would be able to maintain records on direct consumer authorization in the event that questions arise in the future.

Additionally, there will be thousands of third parties accessing a data provider's API every day, and it would be a significant burden on these data providers to affirmatively contact each consumer each time any third party accesses that consumer's information for the first time. A more effective way to limit potential fraudulent authorizations is to allow data providers to revoke access to third parties if they are made aware of potential fraudulent access or activity as

discussed in Q92.[43] Or for the duration of consent to be limited to a finite period of time and require reauthorization, which is also discussed in Q92.

Q76. Please provide input on the approach the CFPB is considering. Are there any alternative approaches the CFPB should consider? As noted in part III.D.2.i above, the CFPB is considering what role screen scraping should play in the context of a covered data provider's compliance with the rule.

As discussed in the response to Q50, the Bureau underestimates the ease with which a third-party access portal can be developed and implemented. Many data providers, small and large alike, do not currently have an API that could provide consumer information to authorized third parties, particularly in light of the extensive variations that could be associated with each third-party authorization. As discussed in the response to Q73, there could potentially be thousands of different custom permutations over what data can be accessed, which would place a significant burden on data providers. As detailed in the response to Q57, industry standard-setting bodies could create common use cases and data categories that data providers can build their APIs around to meet the needs of the market.

Q77. Please provide input on whether covered data providers have the technical capacity to make information available in terms of the frequency and duration sought by authorized third parties through screen scraping, including whether there are considerations particularly relevant to small entities.

As discussed in the response to Q50, if data providers are required to build and maintain a third-party access portal, the data provider should be permitted to block all screen scraping by third parties. Screen 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 providers to effectively block screen scraping and push usage of safer APIs. Moreover, screen scraping in this context is wholly contrary to the notion of consumer authorization. At its core, this authorization is meant to give the consumer control over the scope of the third party's access to the consumer's information, including the frequency and duration of access; if screen scraping is permitted as an alternative to API access, that tailoring of the consumer's authorization vanishes and a third party could have access to consumer information beyond what the consumer has authorized. Even if a token, rather than the consumer's access credentials, is used, the scope of consumer information that a third party could access could be greater than the scope the consumer could restrict the third party to through authorization for access through a third-party access portal, and a data provider would be unable to prevent access to additional data. In addition, information for accounts other than Regulation E or Regulation Z accounts (mortgages, auto loans, student loans, etc.) could be accessible through screen scraping. Given the scope of the SBREFA Outline, such information would have no additional consumer protections.

[43] This is not to suggest that the burden to stop fraudulent authorizations rests solely with data providers.

Q78. Please provide input on whether covered data providers should be allowed to limit the frequency and duration of authorized third parties' access if covered data providers had to permit screen scraping in order to satisfy their obligations to make information available. How could they do so in a way that both minimizes their costs and does not interfere with a consumer's right to access information?

As summarized in the response to Q77, screen scraping is a fundamentally unsafe method of access that undercuts the core purpose of allowing consumers to limit a third party's access to their information through the scope of the consumer's authorization. As further discussed in the response to Q50, it is difficult and costly for data providers to monitor screen scraping and effectively block it, and many data providers are unlikely to have the capacity to know when, and in what volume, a third party engages in screen scraping. Even for larger data providers, it is expensive to differentiate and block automated web scraping while not inadvertently blocking real consumer traffic. Distinguishing the two has only become more difficult as third parties now repeatedly modify their automated scripts to appear more human and bypass efforts to restrict screen scraping.

Q79. Please provide input on the proposal the CFPB is considering. What alternative approaches should the CFPB consider?

As discussed in Q73, authorization should be obtained directly from the consumer, rather than from the third party.

The SBREFA Outline's proposal to require data providers accept evidence of authorization from the third party, rather than requiring evidence of authorization directly from the consumer, creates a greater likelihood of instances in which a data provider would need to clarify the scope of the authorized third party's request with the consumer, as well as increases the risk for an unauthorized third party to obtain consumer data fraudulently. These circumstances could be identified more quickly and addressed more readily when the data provider directly obtains evidence of authorization from the consumer, rather than from the third party. Additionally, building functionality in systems to potentially handle thousands of different custom permutations of authorized data access and what limits are placed on that access, would be a significant technological hurdle and extreme financial burden for data providers to overcome.

Q80. Please provide input on the approach the CFPB is considering with respect to authenticating the identity of the authorized third party. What alternative approaches should the CFPB consider? Is there other information that covered data providers might need before being obligated to make information available to a third party?

The SBREFA Outline's proposal that covered data providers would need to make information available to a third party, upon request, when it receives information sufficient to authenticate the identity of the third party, in addition to evidence of authorization and information needed to identify the scope of information requested, does not recognize that many data providers have agreements with specific third parties they have performed due diligence on and assessed the risk of. Today there are thousands of third parties that may seek to access consumer information from a data provider. Third parties can include data recipients, as well as intermediaries like data

aggregators that facilitate access between numerous data providers and data recipients. Data providers incur incremental costs for each third party - data recipient and data aggregator alike - with whom they integrate directly with; this direct integration includes support, testing, managing of complaints and issues, third-party oversight, and all legal and compliance work.

The Bureau's proposal fails to recognize the different degrees of assessment required for third parties whom data providers already have established relationships with, and entirely new entities that the data providers have not performed due diligence on. Different third parties have different attendant risks, so even if a data provider can authenticate the identity of that third party, it is imperative that data providers maintain the ability to decide with whom they will connect and preserve the right to diligence a third party before making information available to that third party. Further, time, place, and manner restrictions are needed to manage the risk associated with each party.

Q81. Please provide input on whether it would facilitate compliance or reduce costs to covered data providers and authorized third parties if covered data providers were required to follow certain specific procedures in authenticating an authorized third party's identity. Please provide input on what models the CFPB could look to for prescribing such procedures. Do all covered data providers require a uniform set of information to authenticate an authorized third party's identity prior to making information available to the authorized third party?

As discussed in the response to Q72, the Bureau should provide more information on how data providers would be expected to verify a third party's identity. Outside of bilateral contracts between data providers and third parties or an industry registry of authorized third parties, it is going to be difficult for data providers to reasonably operationalize the requirements to directly verify the identity of the potentially thousands of third parties, including potentially very small third parties from a variety of different industries, a data provider will be interacting with. Today, data providers typically verify the completeness of third-party authorizations through contractual obligations between data providers, data aggregators, and data recipients. The Bureau should engage with and support the efforts by industry standard-setting bodies to develop procedures for authenticating an authorized third party's identity that are feasible in the market and reflect the realities of the relationship between data providers and third parties. These procedures should be driven by market participants and flexible to address a continually evolving landscape, rather than be statically prescribed by the Bureau through regulation.

Q82. Should covered data providers be required to make information available to third parties when they know the information requested is inaccurate?

As summarized in the response to Q44, data providers already perform regular assessments to validate, or correct, information in data providers' control. Data providers do not knowingly provide inaccurate information, nor do they have in interest in doing so; in fact, data providers already have obligations to correct inaccurate information once they determine that they have inaccurate information in their possession. An obligation on data providers to make information available to third parties when the data provider knows the information requested is inaccurate is

illogical, because if a data provider is aware information is inaccurate, the data provider would correct the information before sharing such information with a third party.

Q83. Do covered data providers have systems in place that have the capability to both identify information as inaccurate and then withhold such inaccurate information from transmission to an authorized third party? Please provide input on costs to covered data providers if such a system would need to be developed.

As summarized in the response to Q44, data providers in the ordinary course of business already perform assessments to validate, and to correct, information in data providers' control. Data providers do not knowingly, and have no interest in knowingly, provide inaccurate information; in fact, data providers already have obligations to correct inaccurate information once they determine that they have inaccurate information in their possession. Therefore, data providers should not need to have systems in place that have the capability to identify information as inaccurate and then withhold such inaccurate information from transmission to an authorized third party, because once the data provider is aware of the inaccuracy of any information, the data provider would correct that inaccuracy. Further, consumers are already able to contact their financial institutions to correct inaccurate data through the contact information provided as part of the account agreement and opening documentation.

Q90. If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties (see part III.D.2.i above), how would third parties using screen scraping comply with limits on collection? Would third parties employ filters or other technical solutions to limit collection?

Screen scraping should not be a permissible method for third parties to access consumer information from a data provider. Screen scraping is a fundamentally unsafe method of access, and making information available to a third party through screen scraping rather than a third-party access portal wholly undermines attempts to empower consumers. If screen scraping is permitted as an alternative to API access, that tailoring of the consumer's authorization vanishes and a third party could have access to consumer information beyond what the consumer has authorized, negating any attempt to limit collection and increasing risk to consumers.

Q91. Please provide input on the approach the CFPB is considering to limit duration and frequency according to what is reasonably necessary to provide the product or service the consumer has requested. What alternative approaches should the CFPB consider? How could the CFPB reduce costs and facilitate compliance for small entities?

CBA believes that a third party's right to access consumer financial data should be limited in duration and frequency. In drafting a final rule, the Bureau should consider providing guidance on what "reasonably necessary" means and provide examples of practices that would and/or would not be considered "reasonably necessary to provide the product or service the consumer requested" tailored to the product or service offered. The Bureau should also consider that the amount of time that is reasonably necessary may necessarily differ by use case, for example, a data recipient collecting information for the underwriting of a mortgage will need access for a lesser duration and frequency than a website or mobile application offering financial planning

tools. Regardless, the Bureau should consider how long it has been since the consumer last actively engaged with the product or service as a key indicator, as the longer the period of inactivity, the less it is reasonably necessary to maintain access.

Q92. Please provide input on the approach the CFPB is considering that would establish a maximum durational period for all use cases, along with any alternative approaches the CFPB should consider. Please provide input on the length of the maximum durational period, including whether certain use cases should have shorter or longer maximum durational periods.

CBA would support a rule that permits data providers to establish a maximum durational period. The financial services industry should be allowed to establish durations based on the use case for instances when a consumer is actively using the service. However, when there is inactivity, the Bureau could impose restrictions on access by data recipients after a certain period of time has passed and the user has become 'dormant'. This dormancy period will likely differ based on the underlying facts (for example, if a consumer has not used a third party's app in several months, if the consumer has deleted the third party's app, or for a one-time mortgage refinance) six months is likely appropriate, and, as discussed in more detail in Q93, below, a consumer can re-authorize access after expiration. For other use cases, 12 months may be appropriate. Additionally, CBA urges the Bureau to allow data providers to have the ability under the rule to revoke a third party's authorization to protect consumers. For example, if there is a suspected data breach on the third party's system that the data provider bank is made aware of, the data provider should be able to revoke the third party's access in order to help protect consumer data. Similarly, a data provider should be able to revoke a third party's access if the data provider is made aware of fraudulent access or activity.

Q93. If the rule were to require third parties to obtain reauthorization after a durational period has lapsed, how could the CFPB reduce negative impacts on consumers and unnecessary costs on authorized third parties? For example, should the CFPB consider proposals that would allow authorized third parties to:

- **Seek reauthorization, either before authorization lapses, or within a grace period after authorization lapses?**
- **Establish a presumption of reauthorization, subject to a consumer's ability to opt out of the presumption, based on the consumer's recent use of a product or service? If so, what should be considered "recent" use?**
- **Require all authorized third parties to obtain reauthorization on the same day or during the same month each year, for all consumers?**

In this question the Bureau references reducing unnecessary costs on authorized third parties, but does not acknowledge that most of the cost of authorization and reauthorization will be borne by data provider banks, who have significant consumer privacy, security regulatory, and oversight compliance requirements whenever they release consumer financial data. CBA refers the Bureau to Q12, Q13, and Q16 for more information on CBA's proposal to continue current industry practices for authenticating consumers and consumer authorization to data provider banks, rather than consumer authorization being provided to data holding banks by third parties.

Assuming the Bureau agrees with CBA and proposes to follow current industry practices with regard to consumer authentication and authorization, CBA proposes that consumer re-authorization to release data to a third party would be done through data providers, not through third parties (though, CBA would support an additional, separate, requirement for the consumer to also re-authorize the third party's use of the data).

CBA proposes that a consumer's consent for a specific third party to access their data, or the maximum durational period before re-authorization is required, be determined based on the use case. For certain use cases (for example, if a consumer has not used a third party's app in several months, or if the consumer has deleted the third party's app, or for a one-time mortgage refinance) six months is likely appropriate. For other use cases, 12 months may be appropriate.

In general, CBA supports the proposition that authorization and re-authorization control should reside with the consumer, through their data holding bank.

Q94. Please provide input on the approach the CFPB is considering that would require authorized third parties to provide consumers with a mechanism through which they may revoke the third-party's access to their information. Please provide input on the costs associated with providing consumers a revocation mechanism. Please provide input on any alternative approaches the CFPB should consider, and how the CFPB could reduce costs and facilitate compliance for small entities.

In general, and as discussed in Q93, CBA supports the proposition that authorization and re-authorization control should reside with the consumer, through their data provider. Consumers should also have the ability to revoke authorization at any time, through their data provider. Data providers have pre-existing relationships with consumers and robust data security practices and requirements around sharing consumer data. Additionally, and as discussed in Q92, CBA urges the Bureau to allow data providers to have the ability under the rule to revoke a third party's authorization to protect consumers.

Q95. Please provide input on whether covered data providers should also be required to provide consumers with a mechanism by which they may revoke third-party authorization, and the costs and benefits of such an approach. Is it feasible to require covered data providers to provide revocation mechanisms where screen scraping is used?

As discussed in Q92 and Q94, CBA urges the Bureau to allow data providers to revoke a third party's authorization to protect consumers in certain situations. Revocation mechanisms are increasingly difficult and very costly to implement in instances where screen scraping is permitted. Although it is technically feasible to block an IP address that a third party engaged in screen scraping is using to access a data provider's site, the data provider runs the risk of potentially blocking legitimate IP addresses because screen scraper IP addresses are often crafted to appear like a normal consumer's IP address.

Q96. Please provide input on whether authorized third parties should be required to report consumer revocation requests to covered data providers. What would be the challenges or costs anticipated from such a requirement?

As discussed in Q92 and Q94, CBA urges the Bureau to allow data providers to revoke a third party's authorization to protect consumers in certain situations. CBA does not support third parties obtaining consumer revocations, even if they are reported to data providers. A consumer's revocation of a third party's access should come to the data provider directly from the consumer (and, if a consumer chooses, notice should be provided by the consumer, separately, to the third party). Consumer revocations provided to data provider banks by third parties would be less secure than current practices and would force data providers to create less secure, unnecessary, and costly new systems.

Q98. Please provide input on the standard the CFPB is considering for defining secondary use of consumer-authorized information. In providing this input, please describe any guidance the CFPB should consider to clarify the applicability of the standard to particular uses or any alternative standards the CFPB should consider.

CBA does not support the Bureau's current definition of "secondary use" because CBA does not support the Bureau's current working definition of a "data recipient." As stated above in response to Q5, the Bureau's working definition of a "data recipient" includes anyone that provides (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer. This could include nonbank third parties or other banks that are not the current data providers of the consumer's information. However, there is a huge chasm in the consumer data security safeguards and protections between third parties and data providers. As discussed later in this letter, data provider banks are subject to the Safeguards Rule as well as the GLBA and Regulation P, as well as federal and state oversight. Nonbank third parties are not. Thus, the restrictions the Bureau is considering placing on the secondary use of consumer data by data recipients should be differentiated by whether the data recipient is a federally- or state-chartered bank, or whether they are a nonbank entity.

Q99. Please provide input on the various approaches the CFPB is considering to limit third parties' secondary use of consumer-authorized information and any alternative approaches the CFPB should consider. For example:
• What specific protections could be included in an opt-in or opt-out approach to ensure that consumers are informed about their choices and the corresponding risks in a way that balances costs for third parties? Should the rule include requirements or restrictions on the timing and format of opt-in or opt-out requests to prevent the use of potentially misleading practices aimed at soliciting the consumer's consent, such as a prohibition on pre-populated opt-in requests?
• How could the CFPB design such approaches to facilitate compliance by small entities? Should the CFPB propose to include a standard for defining "high risk," or provide a specific list of uses that it deems to be "high risk," or both?

The proposed definition of "secondary use" (a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested including the third party's own use of consumer data and the sharing of data with downstream entities") is too restrictive and could limit or prohibit consumer-friendly innovation by data provider banks. Since data provider banks may be a "third party," they may be able to use a consumer's own information internally, subject to rigorous information security rules and protocols, to provide products and services that would benefit the consumer.

Potential secondary uses of consumer financial data by third parties that are not currently subject to information security rules and federal oversight and examinations on the retention and use of consumer data, however, could pose harm to consumers. CBA supports limitations on downstream uses of consumer data, particularly the monetization of consumer data by third parties whether or not that data is "de-identified." CBA would support a prohibition on the monetization of consumer financial data, or the sale of consumer financial data to third parties that the data provider does not have an API or contractual agreement with. The sale of consumer financial data that is not connected to the product or service for which the consumer engaged with a third party should also be prohibited. If the Bureau does not prohibit downstream parties from using consumer data beyond what is reasonably necessary, they should adopt a required consumer opt-in regime. The Bureau should also publish model disclosures so consumers are aware of the full extent of how their data is, or may be, used.

Q100. Please provide input on whether the rule should include a prohibition on third parties' use of consumer-authorized information that is not otherwise necessary to obtain the product or service requested by the consumer. Please provide input on the costs and benefits of that approach.

In general, CBA supports limitations on downstream uses of consumer data, particularly the monetization of consumer data by third parties. However, the proposed definition of "secondary use" (a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested including the third party's own use of consumer data and the sharing of data with downstream entities") is too restrictive and would severely limit or prohibit consumer-friendly innovation by data provider banks, where banks would be able to use a consumer's own information internally, subject to rigorous information security rules and protocols, to provide products and services that would benefit the consumer.

Of the approaches listed by the Bureau in the SBREFA Outline, CBA would generally support (4), but notes that it is unclear what the Bureau means by "certain high risk secondary uses."

Q102. Please provide input on whether the rule should allow consumer information that has been de-identified to be used by third parties beyond what is reasonably necessary to provide the requested product or service? If so, by what standard should consumer information be considered "de-identified"?

In general, CBA opposes any data shared outside of an API or other direct contractual agreement. CBA supports limitations on downstream uses of consumer data, particularly the

monetization of consumer data by third parties whether or not that data is "de-identified." However, as stated above, in response to Q100, the proposed definition of "secondary use" (a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested including the third party's own use of consumer data and the sharing of data with downstream entities") is too restrictive and would severely limit or prohibit consumer-friendly innovation by data provider banks, where banks would be able to use a consumer's own information internally, subject to rigorous information security rules and protocols, to provide products and services that would benefit the consumer. If the Bureau does not prohibit third parties from using consumer data beyond what is reasonably necessary, they should adopt a required consumer opt-in regime with model disclosures so consumers are aware of the full extent of how their data is, or may be, used.

Q111. Please provide input on the approach the CFPB is considering regarding data security. What alternative approaches should the CFPB consider? Would a general requirement to develop, implement, and maintain a comprehensive written data security program appropriate to a third party's size and complexity, and the volume and sensitivity of the consumer information at issue, provide sufficient guidance? How could the CFPB reduce costs and facilitate compliance for small entities?

Protocols, policies, practices, and oversight should be consistent throughout the data access ecosystem regardless of which entity is holding or sharing consumer data. Banks take consumer security seriously and must abide by the GLBA's safeguards framework, as implemented by the FTC in its Safeguards Rule and by the prudential regulators in the Safeguards Guidelines, along with Regulation P, as they apply to consumer accounts and consumer data. Banks are also subject to significant third-party oversight requirements for entities the bank engages with. All parties in the data ecosystem that hold or maintain consumer data should be held to the same data security standards and appropriate oversight and the Bureau should evaluate the risk posed to consumers in not conducting supervisory activities.

Q112. For third parties: what data security practices do you currently apply to consumer data? Do you tailor your information security approach to an existing legal or industry standard, such as the safeguards framework, and if so, which one(s)? Would you follow the Safeguards Rule or the Safeguards Guidelines if either were incorporated as an option for complying with any data security requirement under the CFPB's rule? Are there alternative data security standards that you believe adequately address data security, and how would implementation costs compare?

As summarized in the response to Q111, protocols, policies, practices, and oversight should be consistent throughout the data access ecosystem regardless of which entity is holding consumer data. To promote consistent protection, all entities operating in the data access ecosystem should be required to comply with the Safeguards Rule or Safeguards Guidelines issued under GLBA. Additionally, to ensure that third parties are meeting their required data security standards, the Bureau should clarify what type of oversight these third parties will be subject to and how data providers can confirm for themselves that third parties are following the Safeguards Rule or the Safeguards Guidelines. The Bureau should work closely with other regulators to ensure that similar importance is consistently placed on data security.

Q119. Please provide input on the approach the CFPB is considering regarding a record retention requirement, along with any alternative approaches the CFPB should consider. Please provide input about the costs to covered data providers and authorized third parties that would be associated with such a requirement. What types of records would be relevant in assessing whether a data provider or authorized third party was complying with the rule? How could the CFPB reduce costs and facilitate compliance for small entities?

In order to provide accurate information on increased costs for record retention, the Bureau must provide more clarity on what types of records it would be asking data providers to maintain – above and beyond what they are already required to retain under the myriad of regulations to which banks are already subject to, including: Regulation B, Regulation C, Regulation E, Regulation V, and Regulation Z. Any obligation of data providers to maintain records should be in line with pre-existing recordkeeping requirements that are applicable to the relevant underlying records, and any records beyond what is required under applicable regulations that need to be maintained should be maintained by data providers for the same amount of time. As the plain language of the statute makes clear, "[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,"[44] so an additional record retention requirements beyond what is already required under applicable regulations would be beyond the authority granted to the Bureau under Section 1033.

Q120. Should covered data providers and authorized third parties be required to maintain policies and procedures to comply with their obligations under the rule, beyond the areas already identified in this Outline? What costs would be associated with maintaining policies and procedures?

As noted in the response to Q119, many data providers are already subject to record retention requirements with respect to many products and services that they offer, and have already built out the necessary policies and procedures to comply with those obligations. However, nonbank authorized third parties may not have the same record retention obligations that covered data providers have under other laws and regulations. To ensure compliance by all parties throughout the data access ecosystem, it is imperative that authorized third parties maintain records to demonstrate their compliance with the obligations under an eventual Section 1033 rule and that they have the necessary policies and procedures in place to effectuate retention of necessary records and consumer protections, consistent with timelines otherwise provided for in relevant regulations.

Sincerely,

Brian Fritzsche
Vice President, Regulatory Counsel
Consumer Bankers Association

Shelley Thompson
Vice President, Associate General Counsel
Consumer Bankers Association

[44] 12 U.S.C. § 5533(c).