January 25, 2023

Via mail:Financial_Data_Rights_SBREFA@cfpb.gov
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Consumer Access to Financial Records, Small Business Regulatory Enforcement Fairness Act Review

I. Introduction

The National Consumer Law Center (on behalf of its low-income clients) (NCLC) and U.S. PIRG are pleased to submit these comments in response to the Consumer Financial Protection Bureau (CFPB)'s Outline of Proposals and Alternatives Under Consideration to Implement Section 1033 of the Dodd-Frank Act, issued pursuant to Small Business Regulatory Enforcement Fairness Act (SBREFA) on October 27, 2022. The CFPB has requested comment on 149 questions in its Outline of Proposals. Our comments address a limited number of these questions that, as a consumer advocacy group, we believe we have some useful input to offer or would like to indicate our position on a proposal.[1]

II. Scope

Questions 1 through 11 deal with scope issues. In general, we support a broad scope and limited exceptions to coverage under Section 1033.

Question 1 asks whether any of the requirements of certain other statutes, as identified in Appendix C of the SBREFA duplicate, overlap, or conflict with the CFPB's proposals under consideration.

As discussed in our comments in response to the CFPB's Advanced Notice of Proposed Rulemaking (ANPR) in this Section 1033 rulemaking,[2] we believe that several other statutes within the CFPB's jurisdiction will apply to consumer-authorized data or when such data is used for certain purposes.

[1] These comments were drafted by Chi Chi Wu, Carla Sanchez-Adams (government benefits card section), and April Kuehnhoff (coverage of debt collectors) with editorial oversight by Lauren Saunders.

[2] National Consumer Law Center, Comments to the CFPB Regarding Consumer Access to Financial Records Under Section 1033 of the Dodd-Frank Act, Feb. 4, 2021, https://www.nclc.org/resources/comments-to-cfpb-in-response-to-anpr-regarding-consumer-access-to-financial-records-under-section-1033-of-the-dodd-frank-act/.

These statutes include the Electronic Funds Transfer Act (EFTA), the Fair Credit Reporting Act (FCRA), the Gramm Leach Bliley Act (GLBA), and the Truth in Lending Act (TILA).

The requirements of some of these statutes will overlap with the CFPB's proposals under consideration. For example, with respect to the ability of consumers to dispute inaccuracies, both the FCRA and EFTA give consumers the right to lodge disputes, 15 US.C. §§ 1681i(a), 1693f. The FCRA imposes accuracy requirements on both consumer reporting agencies (CRA), 15 U.S.C. ¢ 1681e(b), and data furnishers, 15 U.S.C. § 1681s-2(a). For credit cards, the Truth in Lending Act (TILA), which incorporates the Fair Credit Billing Act (FCBA), provides dispute rights, 15 U.S.C. §§ 1643, 1666, 1666i. If the scope of Section 1033 rules is extended to mortgages, the Real Estate Settlement Procedures Act (RESPA) provides for dispute rights in the form of Qualified Written Requests, 12 U.S.C. § 2601. And if the scope is extended to debt collectors, the Fair Debt Collection Practices Act (FDCPA) also provides for a limited right to validation, 15 U.S.C. § 1692g(b).

There could also be overlapping notice requirements. For example, there may be overlap between Gramm Leach Bliley Act (GLBA) privacy notices and the authorization disclosures contemplated by the CFPB's proposal.

However, the potential overlap between the Section 1033 proposal and these statutes should not present a major hurdle for covered data providers, data aggregators, or data recipients. Many covered persons, including smaller entities, must comply with multiple consumer laws. For example, a small depository institution may need to comply with not only EFTA, GLBA, and the FCRA with respect to deposit accounts, but for credit accounts also TILA and the Equal Credit Opportunity Act (ECOA). They must also generally comply with state and federal prohibitions against unfair, deceptive or abusive acts or practices.

The statutes listed above also may have overlapping requirements, with which smaller entities have dealt for many years. For example, both the FCRA, 15 U.S.C. § 1681m(a) and the ECOA, 15 U.S.C. § 1691(d)(2), require lenders to provide an adverse action notice when a creditor rejects an applicant based on a consumer report. Small lenders have been required to provide adverse action notices for decades. Of course, one measure that has helped lenders comply with these overlapping requirements is model notices that combine the requirements of both statutes. The CFPB could provide model forms and guidance on how to comply with requirements of both the Section 1033 rule and other statutes.

Question 5 asks for input on the approach the CFPB is considering with respect to which data providers should be covered by the Section 1033 rule. It specifically asks whether the CFPB should consider covering (1) providers of government benefit accounts used to distribute needs-based benefits programs and (2) credit products that are not Regulation Z credit cards.

In general, we support a broad scope of coverage that would include not only government benefits card providers and closed-end creditors, but also debt collectors, non-credit data furnishers, CRAs, and other covered persons. Consumers should always have the right to access information about themselves held by a covered person, with very limited exceptions. This is the underlying principle of state privacy laws such as the California Consumer Privacy Act, and we believe it should be a fundamental consumer right. At the same time, it is important to ensure that that consumers' privacy is not violated in the name of the right to access their data, that consumers' consent to share data is voluntary and knowing, and that minimum amount of data necessary for the purpose is shared, and is shared in a way that consumers would expect.

More concretely, as we noted in our Feb. 2021 ANPR comments, consumer-authorized data has the ability to provide alternative credit underwriting models that could challenge the oligopoly of the nationwide CRAs, *i.e.* Equifax, Experian and TransUnion. Much of the attention on alternative data and Section 1033 has focused on deposit account transaction and cashflow data, which appears to be very promising. However, companies might be able to build other types of competitors to CRAs using consumer-authorized data. For example, Certree and Argyle have emerged as potential competitors to The Work Number, a payroll data CRA owned by Equifax; these competitors use "lockers" into which consumers can supply their payroll information.[3] One could easily imagine a competitor to the nationwide CRAs that uses similar "lockers" for credit account data, thus setting up a CRA that relies on consumer-authorized data.

1. Government Benefit accounts

We generally support coverage of Section 1033 to providers of government benefit accounts used to distribute needs-based benefits programs, especially to EBT accounts.

In 2021, about 41.5 million people across the country participated in the Supplemental Nutrition Assistance Program (formerly known as Food Stamps).[4] SNAP benefits are distributed and administered through the Electronic Benefit Transfer (EBT) system to eligible participants. EBT has been the sole method of SNAP issuance in all states since June of 2004,[5] and some states also use EBT cards to issue Temporary Assistance for Needy Families (TANF) or other state administered financial assistance.[6]

State and territorial governments currently contract with private companies, known as EBT processors, to administer EBT cards, with two of the processors owning roughly 95 percent of the state contracts between them.[7] EBT processors are not required to provide SNAP beneficiaries with access to information about their accounts electronically, and households that receive these benefits often experience data unavailability, slow connectivity, and other obstacles related to ease of access to account information. For example, if an EBT accountholder needs to know their account balance, they must: (1) call a number and spend considerable time navigating through a voice response system; (2) visit a website or app maintained by the EBT processor (assuming they have internet access, which many do not); or (3) make a purchase to see balance information on a retail receipt.

However, people who receive SNAP need access to vital information like account balance and transaction history more acutely than other households with larger financial cushions and without the added friction. These households need to know their balances to the penny and the minute in order to manage their expenses.

---

[3] Andrea Vittorio, Startups Take on Equifax, Experian Over Payroll Data Dominance, Bloomberg Law, Dec. 15, 2022, https://news.bloomberglaw.com/privacy-and-data-security/startups-take-on-equifax-experian-over-payroll-data-dominance

[4] https://datacenter.kidscount.org/updates/show/296-snap-in-2021 Kids Count Data Center by the Annie E. Case Foundation

[5] https://www.fns.usda.gov/snap/ebt.

[6] https://fns-prod.azureedge.us/sites/default/files/resource-files/ebt-contract-procurement-summary-20221215.pdf.

[7] *Id.*

Additionally, EBT cardholders need immediate access to balance and transaction information especially in the context of fraud and theft. Recently, EBT cardholders have been targeted by criminals who "skim" account information and PINs and then deplete the accounts of all funds belonging to the recipients. This problem is so endemic that even the USDA issued a policy memo on EBT card skimming prevention with tools and resources to prevent and identify the fraud.[8] Unfortunately, most of the recommendations issued by the USDA put the onus on consumer education and consumer prevention, when there is little that consumers can do. As a result, these consumers need more timely access to their accounts to identify fraud and identity theft, take the preventative measures recommended, and dispute account errors.[9]

EBT was created with the intent of introducing a government benefits payment experience similar to private-sector debit cards. However, EBT accounts are the only major electronic funds transfer accounts that are not covered by protection against unauthorized charges and errors under the EFTA, Regulation E, or other federal consumer laws. For this reason, it is imperative that EBT cardholders who have been victimized by theft have immediate access to balance and transaction information so that they can spot any problems immediately and freeze their accounts as soon as possible. They should be able to obtain greater access to their account information as they attempt to recover some of their stolen money.

In some states, third-party providers have entered the market to provide low-income families with opportunities to access their EBT account balances and view their transaction histories in a faster, easier, and arguably more reliable way. These third-parties are essentially data aggregators, providing services to EBT accountholders in a similar fashion to the other data aggregators and fintechs covered by this rulemaking.

At the same time, third-party access to the information in EBT accounts poses unique threats to EBT cardholders. With other accounts, Regulation E protects consumers if they share their account credentials with a data aggregator and those credentials are stolen, leading to unauthorized charges.[10] But because EBT accounts are not covered by EFTA and have no error resolution dispute rights for unauthorized transfers under EFTA, we are concerned that consumers who choose to share their EBT information with data aggregators may not have any protection if their information is not kept securely.

The Bureau should protect these EBT accountholders by using all available authorities to ensure that data aggregators are subject to data security, data privacy, and UDAAP protections. The Bureau should also include data aggregators and data recipients that access EBT card information in a larger participant rulemaking to ensure that the CFPB is able to supervise them and prevent or remedy any consumer harm. We also urge the Bureau to work with the Department of Agriculture, the Department of Health

[8] https://www.fns.usda.gov/snap/snap-tanf-ebt-card-skimming-prevention.

[9] Some of the preventative measures highlighted by the USDA include freezing or locking cards and transaction and PIN change alerts. *See* Appendix A: Card Security Options Available to Households available at https://fns-prod.azureedge.us/sites/default/files/resource-files/ebt-card-skimming-prevention.pdf.

[10] The CFPB has made clear that if the EFTA's unauthorized transfer protections apply if a fraudster initiates a transaction using stolen credentials or if the consumer is fraudulently induced into sharing account access information. See CFPB, Electronic Fund Transfer FAQs, Error Resolution: Unauthorized EFTs, Q 4, 5, 6, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#unauthorized-eft. Consumer negligence also plays no role, and financial institutions cannot include provisions in their account agreements waiving EFTA protections. *See id.* Q 7, 8.

and Human Services, states and Congress to give EBT cardholders the same protection that other consumers have under the EFTA.

2. Credit products other than credit cards

We support the expansion of the CFPB's Section 1033 proposal to closed-end credit products such as mortgages, auto loans, installment loans, and more. As discussed above, such access would be necessary for the creation of competitors to the nationwide CRAs. Furthermore, the text of Section 1033 is not limited to either deposit account data or credit card data, but includes any "consumer financial product or service."

3. Risk scores other than credit scores

As discussed more fully in our February 2021 comments to the ANPR, the CFPB should adopt rules to give consumers the right to access any risk score, predictor, or recommendation that a covered person used in connection with providing the consumer a financial product or service. It should also give consumers access to any behavioral data sold by the nationwide CRAs to covered persons for marketing purposes.

4. Payroll services providers

As discussed above, two competitors have emerged to Equifax's The Work Number, which provides payroll data collected from employers. While the scope of Section 1033 is unlikely to extend to employers, the CFPB could include payroll data furnishers within the scope. These include companies such as ADP that furnish information to the Work Number.[11] Since The Work Number is used for credit underwriting,[12] furnishers of data to that CRA could be considered covered persons.

5. Information from debt collectors

The CFPB should include debt collectors (as defined in the FDCPA, 15 U.S.C. § 1692a(6)) as covered data providers. Debt collectors should be required to make available to a consumer or an authorized third-party any information that pertains to a debt allegedly owed by the consumer. This would promote the purposes of the FDCPA, in particular the right to validation under § 1692g(b). As the CFPB has previously noted with respect to § 1692g(b):

> [T]he FDCPA provides no explanation of these requirements, and courts have interpreted them in various ways. As a result, debt collectors vary in the level of documentation they obtain and provide to consumers to verify a debt, with many collectors currently not reviewing or providing copies of underlying account documentation in response to disputes.[13]

[11] See The Work Number – ADP Verification Services, October 1, 2013, https://controller.iu.edu/services/payroll-processors/central-payroll-office-resources/TheWorkNumber%20Central%20Office%20Procedure.pdf

[12] The Work Number, Instant Verification of Employment and Income for Mortgage, https://theworknumber.com/solutions/industries/mortgage-verification (visited January 19, 2023).

[13] Consumer Financial Protection Bureau, Small Business Review Panel for Debt Collector and Debt Buyer Rulemaking: Outline of Proposals Under Consideration and Alternatives Considered p. 11 (June 28, 2016), available at: https://files.consumerfinance.gov/f/documents/20160727_cfpb_Outline_of_proposals.pdf.

Although the CFPB recognized this problem and proposed solutions,[14] no solutions were implemented as part of Regulation F.

Covering debt collectors under Section 1033 will provide critical consumer protections by helping consumers determine whether the right debt collector is contacting the right person to collect the right amount. Currently, there is no guarantee that disputing consumers will receive any meaningful information to help them answer questions about the alleged debt beyond the required validation information.[15] Indeed, some courts have held that "verification of a debt involves nothing more than the debt collector confirming in writing that the amount being demanded is what the creditor is claiming is owed."[16] Section 1033 represents an opportunity to establish a right for consumers to access information that a debt collector possesses about the alleged debt. It could also specify for debt collectors what information must be provided to consumers.

Including debt collectors within the scope of Section 1033 should clearly stipulate that debt collectors have an obligation to provide information about the alleged debt after the validation period.[17] Other sections of the FDCPA still protect consumers who dispute debts outside of the validation period, e.g., § 1692e(8), as well as other statutes such as the FCRA.

Question 6 and 9 ask for input about exemptions for data providers. Question 6 asks about exemptions generally, while Question 9 asks for input on whether and what asset size or activity level would be an appropriate metric for a possible exemption for covered data providers that are depository institutions, and that are not depository institutions.

We believe that the CFPB should not provide any exemptions based on size for depository institutions, so long as the institution has the ability to retain a third-party core processor for its banking systems that offers third party portal access under a certain pricing threshold. This threshold should be based on the size of the small institution, *e.g.*, if there is a core processor that will provide the institution with third-party portal access for an annual fee of 0.1% of asset size. With respect to credit card accounts, we are unaware of any credit card lenders who qualify as small financial institutions, i.e., less than $750 million in assets.[18]

As the CFPB knows and discusses on page 55 of the SBREFA Outline, most smaller depository institutions use third-party core processors for their back-office support to process daily banking transactions, as well as post updates to accounts and other financial records. Examples of core processors include Fiserv, FIS, and Jack Henry, which together provide core systems for just over 71 percent of U.S.

---

[14] *Id.*

[15] *See also* National Consumer Law Center, Fair Debt Collection § 9.11.3 (10th ed. 2022), updated at: www.nclc.org/library (collecting cases discussing collector's verification of debts).

[16] *Clark v. Cap. Credit & Collection Servs., Inc.*, 460 F.3d 1162, 1173–74 (9th Cir. 2006), *quoting Chaudhry v. Gallerizzo,* 174 F.3d 394, 406 (4th Cir.1999).

[17] "Validation period" is defined at 12 C.F.R. 1006.34(b)(5).

[18] See Institute for Local Self-Reliance, Distribution of Credit Card Loans by Banks Size, 1994-2018, May 15, 2019 https://ilsr.org/distribution-of-credit-card-loans-by-banks-size-1994-2018/ (chart appearing to show that by 2018, no "small banks" were credit card issuers)

depository institutions.[19] These companies are certainly not small entities since in FY 2021 they had revenues of $16 billion (Fiserv),[20] 13.9 billion (FIS)[21] and $1.9 billion (Jack Henry),[22] respectively.

Thus, for example, one of the smallest U.S. depository institutions is Emigrant Mercantile Bank, with an asset size of $3.4 million.[23] Despite its small size, it has an online banking platform, which presumably is supplied by a third-party core processor. Indeed, the Bureau itself recognizes this in its discussion on page 54-56 of the SBREFA Outline of Proposals, as well as page 61 where it states "The CFPB anticipates that the share of small covered data providers providing consumer-authorized data access through third-party access portals will increase, particularly as core banking software providers adopt the technology for their covered data provider customers." In order to ensure the availability of such third-party portal access services, the CFPB should specifically cover third party core processors as covered entities under Section 1033.

The CFPB also notes on page 55 of the SBREFA Outline that core processors often charge a fee to facilitate third-party portal access services, which can range from several hundred dollars for the smallest depository institutions to as high as $50,000 per month for the largest institutions. To prevent this cost from becoming too high for smaller depository institutions, the CFPB could condition Section 1033 coverage on a cost threshold. For example, a threshold of 0.1% of asset size would mean that Emigrant Mercantile Bank would only be required to provide access if there was a core processor willing to provide that bank with third party portal access services for $3,500 annually or less. An institution such as Tioga State Bank, which is a small depository institution with an asset size of $540 million,[24] would be covered if the pricing was $540,000 annually or less – about $45,000 per month, though we expect that the service would be available for far less.

Finally, we note that requiring small depository institutions to provide the same type of consumer-authorized data access as larger banks is actually beneficial for them, provided the cost is not overly burdensome. It pushes back on any narrative that smaller depository institutions have outdated systems and are less technologically advanced than large banks. Smaller depository institutions are already facing significant competitive disadvantages compared to big banks (e.g., more ATMs, name recognition). It would compound the disadvantage to leave smaller institutions out of the technological evolution of consumer-authorized data, including the best way to share that data (i.e., application programming interfaces, see Responses to Question 50 through 56 below).

---

[19] Amber Buker, How Innovative Banks Are Reimagining the Core, Bank Director, July 10th, 2019, https://www.bankdirector.com/issues/how-innovative-banks-are-reimagining-core/

[20] Press Release, Fiserv Reports Fourth Quarter and Full Year 2021 Results, February 8, 2022, https://newsroom.fiserv.com/news-releases/news-release-details/fiserv-reports-fourth-quarter-and-full-year-2021-results

[21] Press Release, FIS Reports Fourth Quarter and Full-Year 2021 Results, February 15, 2022, https://www.investor.fisglobal.com/news-releases/news-release-details/fis-reports-fourth-quarter-and-full-year-2021-results

[22] Press Release, Jack Henry & Associates, Inc. Reports Fiscal 2021 Results, Aug. 17, 2021 , https://ir.jackhenry.com/news-releases/news-release-details/jack-henry-associates-inc-reports-fiscal-2021-results

[23] MX Blog, Biggest U.S. Banks by Asset Size, April 20, 2021, https://www.mx.com/blog/biggest-banks-by-asset-size-united-states/.

[24] Laura Alix, Kate Fitzgerald, Joel Berg, The Best Banks to Work For — under $3 billion of assets, American Banker, November 9, 2021 https://www.americanbanker.com/list/the-best-banks-to-work-for-under-3-billion-of-assets.

Question 11 asks for input on making information available for accounts held by multiple consumers. The CFPB is considering proposing that a data provider would be required to make information available to the consumer who requested the information or all the consumers on a jointly held account.

The CFPB should require data providers to make information upon request available to all consumers on a jointly held account. All of the consumers might need access to data from the account for various purposes, such as payment processing (e.g., Venmo accounts) or credit underwriting. This is especially important for spouses or partners. Such access would be in line with the goals of Regulation B, which requires creditors to furnish information on both account holders as well as authorized users. See Reg. B, 12 C.F.R. § 1002.10. This provision of Regulation B was adopted to ensure that married women had access to the same credit records as their husbands, given that husbands are more likely to be listed as the primary account holder. Requiring data providers to make information to both account holders under a Section 1033 rule would serve similar purposes.

III. Authorization procedures

The next section in the SBREFA Outline, Questions 12 to 21, pertains to the procedures necessary for consumers to authorize third parties (aggregators and recipients) to access consumer information on consumers' behalf. These proposals seek to ensure that these third parties are actually acting on behalf of the consumer. The proposed requirements include: (1) providing an "authorization disclosure" to inform the consumer of key terms of access; (2) obtaining the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and (3) certifying to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information.

Questions 12 and 13 ask for input on these proposals, alternative or additional approaches, and suggestions. Question 18 asks whether the CFPB should provide model clauses and/or forms for some or all of the content of the authorization disclosure. Question 19 asks for input on whether the CFPB should include any particular requirements or restrictions on timing and to prevent the use of potentially misleading practices aimed at soliciting consent, such as a prohibition on pre-populated consent requests. We provide responses to these questions in the following discussion.

One of the most important aspects of a Section 1033 rule is to ensure that, when a consumer provides authorization to a third party to access their data, the consent act is truly knowing, meaningful, and voluntary. Getting this right is critical – if done wrong, we will end up with another data regime in which consumers are captives and our data is a commodity exploited by companies with impunity, much like the nationwide CRAs. We believe the following measures and formats are necessary to ensure that authorization is truly voluntary and that Section 1033 data access ultimately benefits consumers.

<u>Making consent truly voluntary</u>

As the CFPB knows, consumers often provide "consent" unknowingly or as a pro forma matter, without seeing, reading, or understanding what they are consenting to. Consumers often feel they must consent if they want the service and that there is no alternative. How many of us have spent less than 30 seconds scrolling through a long terms of service webpage and clicked "Agree" because we thought we had no choice in the matter?

To combat this lack of choice, the CFPB should require that authorization disclosures include information about the alternatives if the consumer does not consent. Of course, this means the CFPB should also urge data recipients to have such meaningful alternatives. For example, if a lender is using data for credit underwriting and would otherwise approve an application if the consumer has a credit score over 720, the authorization disclosure should say "if you have a credit score of 720 or higher, we may be able to approve your application using your credit score."

And just as critically, the CFPB needs to actually dissuade and take measures to prevent lenders who currently do not use consumer-authorized data from adopting a mandatory requirement for such information for credit approvals.

Another example would be a payment platform like Venmo, for which the authorization disclosure would be required to say "if you do not wish to share your bank account information with Plaid, you can verify your account manually using microtransfers to your bank account (these will be less than $1 each)."

Model clauses and formatting

The formatting and language of the authorization disclosure will be very important. Obviously, it should be a standalone disclosure with no extraneous text. There should be a requirement that the language used in the disclosure be kept at a sixth-grade level. There should be a maximum word count to prevent overly long, dense, and thus hard-to-read text. We highly encourage the CFPB to consult literacy experts on how to ensure that consumers give permission in a knowing manner with adequate understanding, and are not engaged in click-through consent based on boilerplate.

We support the proposal for the CFPB to develop model clauses. The CFPB should also develop model formatting and model interfaces. Such formatting should use toggles for "on-off" authorization, as opposed to click-through boxes, so that consumers can go back and turn off access easily

Any model forms or clauses should have a mobile friendly version, and the Section 1033 rule should require that disclosures must be mobile friendly when made on a mobile phone.[25] Many low-and moderate-income consumers – indeed, many consumers generally – now primarily rely on their mobile phone to view disclosures and websites. That is another reason to mandate the use of toggle slides and not click-throughs from a pop-up screen.

Other issues

The authorization disclosure should include the name of all parties involved: the covered data provider, the data aggregator, and the recipient (user).

As for timing, disclosures should be provided and authorization sought immediately before any information is accessed. Providing the disclosures and obtaining authorization too early uncouples the

[25] *See* Jeff Sovern and Nahal Heydari, Not-So-Smartphone Disclosures (August 12, 2022). St. John's Legal Studies Research Paper No. 22-0010, 2022, available at SSRN: https://ssrn.com/abstract=4188892 or http://dx.doi.org/10.2139/ssrn.4188892 (finding that consumers understood credit card disclosures significantly less well on smartphones).

authorization from the access and risks the consumer forgetting that they had granted authorization to this information.

Question 14 asks which authorization procedures and obligations should apply to the data recipient, the data aggregator, or both parties. Question 20 asks whether the consumer should be provided with a copy of authorization.

The authorization request and disclosures should be provided by the data aggregator, since that is the entity being authorized to access the data. However, the covered data provider should send a separate confirmation so that the consumer is alerted in case an improper or accidental authorization is somehow obtained, or the consumer does not realize they authorized the disclosure of data to a third party.

A consumer should be provided with a copy of the authorization. Furthermore, if there is ongoing access by an aggregator, there should be information on the provider and aggregator's website in the consumer's online account profile that shows the existence of such access, much the way some banks will show which entities are authorized as recipients of Zelle transfers for a consumer's account. Consumers should be able to view what entities have been granted access to their account on an ongoing basis both on the data aggregators' website – where they should see all accounts that the aggregator can access, and which data users get that data – and on the website of the data provider, where they should be able to see all data aggregators that can access that provider's data. Such information should be provided in a mobile friendly format.

IV. Information required to be provided pursuant to Section 1033

The next set of questions discussed the categories of information that would be required to be disclosed pursuant to Section 1033. The CFPB has stated that the categories would include:

- Periodic statement information for settled transactions and deposits;
- Information regarding prior transactions and deposits that have not yet settled;
- Online banking transactions that the consumer has set up but that have not yet occurred; and
- Account identity information.

We only have a comment on the timeframe for what information must be disclosed. The CFPB is considering limiting this timeframe to only the amount of time that a covered data provider makes transaction history available directly to consumers through the provider's financial account management or similar online portal.

Q38 asks for input on how many years' worth of information should a provider be required to make available under Section 1033.

The CFPB should set a minimum number of years' worth of information that a provider must make available, such as two years. We would be concerned that limiting information access to the amount of time a provider makes data available on an online portal would create an incentive for providers to provide less information on such portals.

We suggest a minimum of two years' worth of information in order to not conflict with Section 1033's provision that nothing in the section imposes a duty on a covered data provider to maintain any information about a consumer. 12 U.S.C. § 5533(c). A two-year timeframe avoids any issues because other laws and regulations, such as Regulation Z, 12 C.F.R. § 1026.25(a) and Regulation E, 12 C.F.R. § § 1005.13(b), require retention of records for two years to document compliance with their requirements. Since providers must retain this information, it should be available under a Section 1033 rule whether or not the provider makes it available via an online portal. And the CFPB might be able to mandate even more years of information if the provider furnishes such information to a CRA, given that the Furnisher Accuracy and Integrity Guidelines require furnishers to maintain records for a reasonable period of time in order to substantiate the accuracy of furnished information, see Appendix E to Regulation V, § III(f).

Also, a longer time frame would be helpful to consumers who may need the information in the event of a tax audit or to confirm that a large purchase is within the warranty period. While such information might not need to be available via third party access, a consumer should be able to obtain it directly upon specific one-time request if the data provider has retained it.

Question 85 asks for input on a proposal to require data providers to disclose to consumers or authorized third parties the reason why information is not available, e.g., pursuant to the section 1033(b) exceptions or insufficient identity authentication.

We support a requirement for data providers to provide a statement of reasons when they withhold information that otherwise a consumer might have the right to access under Section 1033. Consumers should always be provided with information, including the reasons, when they are being denied something important so that they are not left in the dark. This is the policy rationale behind the adverse action notice requirements of the FCRA and ECOA, and the same rationale applies when they are denied information to which Section 1033 otherwise entitles them.

V. How and when information would need to be made available

Questions 39 through 87 discuss issues of how and when information should be made available. In this following section, we primarily focus on the issues of identity authentication; the thorny problem of screen scraping; and fees. We discuss the accuracy issues in Questions 48, 82-84 in the next section.

<u>Identity authentication</u>

Questions 39 and 46 discuss requirements for identity authentication as part of considerations for access to information.

Obviously, strong requirements for identity authentication are critical in order to prevent unauthorized access of the very sensitive and valuable information that a covered data provider would be making available under a Section 1033 rule. Data security is crucial. One type of identity authentication we support is two-factor authentication, where the provider sends a code to the consumer's email address or mobile number by SMS. Two-factor authentication is useful in preventing unauthorized access while not presenting overly great burdens on consumers. Strong security measures should especially be required for data aggregators and data users who access information about EBT cards, which, as discussed above, are not protected from unauthorized transfers.

Conversely, the CFPB should also make sure that providers do not require excessive amounts of information or other overly burdensome measures that stymie the ability of consumers to access their own information. We have seen such excessive requirements by the nationwide CRAs, which we described in detail in our May 2022 comments to the CFPB regarding its proposed rule to protect trafficking survivors.[26] We do not want consumers to face similar barriers in accessing information under Section 1033.

Question 75 asks whether a data provider should be required to notify a consumer of a third party's initial access attempt to reduce the risk of potentially fraudulently obtained authorizations. It also asks whether data providers should be required to inform consumers of which third parties are accessing information pursuant to a purported authorization to enable consumers to monitor third-party access to their account.

As discussed in our response to Questions 14 and 20, data providers should be required to notify the consumer when a third party initially attempts to access their information. The provider should send a text or email confirming access, and perhaps should even be required to use two-factor authentication to authorize the access, i.e., the notice could say "to confirm this access, please select approve".

Also, as discussed in our responses to Questions 14 and 20, there should be disclosures on the provider and recipient's website in the consumer's online account profile that shows whether and which third parties are accessing the consumer's information. Such disclosures should be viewable in a mobile format.

Screening Scraping

Questions 50 to 56 discuss third party access to information. These questions focus on screen scraping and how to move away from it. In particular, Question 53 and 54 asks for input on implementing staggered deadlines with respect to a requirement to establish a third-party access portal using data-sharing agreements, i.e., application programming interfaces (APIs). It asks how the CFPB should define different classes of covered data providers that would be subject to different implementation periods and whether the CFPB should use asset size, activity level, or some other metric.

As discussed in our comments to the Section 1033 ANPR, the CFPB should support and encourage efforts to move away from screen scraping, as it is less secure and collects more information than is necessary, including sensitive information. Screen scraping is also more prone to errors. However, the CFPB cannot prohibit screen scraping until all covered data providers permit access to information using APIs. Thus, it is critical for the CFPB to require that data providers move to APIs in an expeditious manner.

Moving to APIs is technically feasible within a short period of time, especially given the presence of voluntary collaborative efforts to establish common standards, formats, and guidelines. We believe that larger providers (asset size over $10 billion) should be required to move to APIs within the next two

[26] Comments of Consumer and Survivor Advocacy Groups re: Prohibition on Inclusion of Adverse Information in Consumer Reporting in Cases of Human Trafficking, Docket No. CFPB–2022–0023/RIN 3170-AB12, May 9, 2022, https://www.nclc.org/wp-content/uploads/2022/09/FCRA_trafficking_comment.pdf (cataloging examples of onerous levels of identification required by the nationwide CRAs that sometimes prevent consumers from placing an identity theft block or obtaining their file disclosures).

years. All other covered data providers except for small entities should be required to move to APIs within five (5) years, and screen scraping banned for non-small entities at that point. And as discussed in our response to Questions 6 and 9, after five years, small depository institutions should be required to move to APIs once there are core processors offering third-party portal access at a reasonable fee.

Question 63 asks for the impact if covered data providers were or were not restricted from charging specific fees under the rule in order to access information through an API.

We strongly urge the CFPB to prohibit covered data providers from assessing any fees to consumers or aggregators for any sort of data access under Section 1033, whether through an API or other means. Fees to aggregators will inevitably get passed on to consumers.

Such fees might prove to be a significant deterrent to a consumer exercising their rights under Section 1033. Consumers should never be charged a fee to obtain information that federal law grants them a right to access.

VI. Accuracy Issues

This section discusses the need to ensure accuracy in the transmission of consumer-authorized data. The CFPB has laid out several approaches it is considering for accuracy standards: (1) requiring a covered data provider to implement reasonable policies and procedures to ensure that the transmission of information through the covered data provider's third-party access portal does not introduce inaccuracies; (2) establishing performance standards relating to the accurate transmission of consumer information through third-party access portals; (3) prohibiting covered data provider conduct that would adversely affect the accurate transmission of consumer information; or (4) requiring a combination of (1) through (3).

Question 66 asks for comment on these approaches.

We support option 4, i.e., "all of the above," as the strongest and best option. From our experience with consumer reporting agencies, both nationwide and specialty CRAs, requiring "reasonable procedures" for accuracy is not sufficient. To achieve maximum possible accuracy, there also needs to be performance standards (option 2) and prohibitions against certain conduct that creates undue risks of inaccuracy (option 3), as well as certain requirements that promote accuracy.

Just as critically, all of the above measures need to apply to authorized third parties to prevent inaccuracies introduced by them. In a later section, the CFPB proposes to require authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the information that they collect. That is necessary but not sufficient.

Question 113 asks for input on this approach.

The CFPB should require more than just reasonable procedures for accuracy. As with covered data providers, the CFPB should require data aggregators to meet certain performance standards, prohibit certain conduct that creates an undue risk of inaccuracy, and impose certain requirements that promote accuracy.

Question 82 and Question 48 ask whether covered data providers should be required to make information available to third parties when they know the information requested is inaccurate.

If a data provider knows that certain information is inaccurate, they should be required to correct the error and then provide the information. There is no excuse for providing information known to be inaccurate, but there is also no excuse for not correcting known inaccuracies. Allowing a data provider to withhold inaccurate information could create a significant loophole to a consumer's right to access that information under Section 1033. Furthermore, other statutory regimes such as EFTA, TILA, and FCRA may require correction of known errors. Certainly, if the same information is furnished to a CRA, such as credit card data to the nationwide CRAs or deposit account data to Early Warning Services, it must be corrected, since the FCRA prohibits furnishing information that is known to be inaccurate. 15 U.S.C. § 1681s-2(a).

If information is disputed as inaccurate but the dispute is not resolved, then such information should not be provided until the dispute is resolved.

Question 116 asks whether authorized third parties should address disputes submitted by consumers.

Yes, the CFPB should require data aggregators to address disputes submitted by consumers to that aggregator. In fact, as discussed in our February 2021 comments to the CFPB's ANPR on Section 1033, data aggregators should be considered consumer reporting agencies if the data is used for an FCRA covered purpose, *i.e.*, credit, insurance, employment, etc. As CRAs, these third parties would be required under Section 1681i(a) of the FCRA to conduct reasonable investigations when a consumer lodges a dispute over the accuracy of information.

VII. Consumer Protections to Govern Third-Party Access

In the section entitled "Third Party Obligations," the CFPB has laid out proposals for consumer protections, *i.e*., guardrails, for when third parties (data aggregators and data recipients) access consumer-authorized information. Questions 88 to 120 ask for input on these proposals. We respond to specific proposals below. In general, we are very supportive and appreciative of the CFPB's consideration of strong proposals for data minimization, duration of access, retention, and deletion. Such protections constitute a core element of what is needed to ensure that Section 1033 and consumer-authorized data provide the benefits that have been promoted, while minimizing potential exploitation and harm.

1. Data minimization

The CFPB is proposing a data minimization standard for third parties accessing consumer-authorized information. Authorized third parties would not be permitted to collect, use, or retain consumer information beyond what is reasonably necessary to provide the product or service the consumer has requested; the CFPB refers to this as "the limitation standard."

Question 88 asks for input on this limitation standard

We strongly support this data minimization limitation standard. It is critically important to ensure that both data recipients and aggregators do not collect more information than is necessary for the purposes

for which the consumer has authorized the data access. As discussed in our February 2021 comments to the ANPR, deposit accounts (as well as credit card accounts) contain a wealth of information about the consumers' income, where they shop and what they buy, their spending patterns and a variety of other sensitive personal information. Credit and debit card data also include location data that can be extremely revealing, *e.g.*, the fact that a consumer purchases a coffee every morning from a certain café at 8 AM could be abused by not only marketers, but actors with bad intent.

Relatedly, data minimization should also require that the data supplied be consistent with consumers' expectations. Third parties should not be allowed to access more data than a consumer would reasonably expect for the given use. Effective consent is obtained only when the consumer understands what they are consenting to.

2. Duration and Frequency

The CFPB is considering proposing that authorized third parties be limited to accessing data under Section 1033 for only as long (duration) and as often (frequency) as would be reasonably necessary to provide the requested product or service. The CFPB is also considering whether to limit data access to a maximum period, after which a reauthorization would be required for continued access.

Questions 91 and 92 ask for input on the proposals for limits on duration, frequency, and maximum time periods.

We strongly support strong limits on the duration and frequency of third-party access to data authorized under Section 1033, as well as a maximum time period after which reauthorization is required. These limits likely depend on what service or product is being requested by the consumer. For example, if a consumer is applying for closed-end credit, the duration would only be a short period of time when the underwriting is occurring (perhaps two weeks) and the frequency would be one-time. If the consumer is applying for open-credit credit, the duration might be a full year and the frequency might be monthly for account reviews, with a requirement to renew authorization after that year. A tax preparation use would be a one-time use to pull information into a tax prep software program. Personal financial management might be more frequent and the duration a full year, with either active use or renewal required after that. With the exception of personal financial management that is actively being used by the consumer and has no secondary uses, we believe that one (1) year should be the maximum amount of time before a reauthorization for access should be required.

Question 93 asks for comments about potential options requiring reauthorization, including (1) requiring third parties to seek reauthorization, either before authorization lapses, or within a grace period after authorization lapses; (2) establish a presumption of reauthorization, with opt out of the presumption, based on the consumer's recent use of a product or service; and (3) require all authorized third parties to obtain reauthorization on the same day or during the same month each year, for all consumers.

We support requiring active reauthorization after the maximum time period has expired. We would oppose a presumption of reauthorization based on recent use, except for personal financial management where the data recipient is not using the information for another purpose. That is because other ongoing uses may have alternative data sources and not need ongoing access to deposit/credit card account data. In addition, other than active use of a personal financial management app, where the access to and need for the data is obvious, the consumer may not be aware of the use of their data and may wish to reconsider it.

For example, a credit card account underwritten with deposit account data for a credit invisible consumer might be an ongoing use with recent activity. However, the consumer should be asked to reauthorize data after a year, because they may have a good credit score and/or history of repayment to the card issuer. In fact, they should also be informed (as discussed in our response to Questions 12 and 13) of any alternatives to granting continued access to data, *i.e.*, "You may not need to continue giving us permission to access your bank account data because your credit score is now above 620/based on your history of on-time payments during the past year."

3. Revocation

CFPB is considering requiring authorized third parties to provide consumers with a mechanism for revoking the third-party's access to their information.

Question 94 asks for input on the idea of a mechanism for revocation

We believe that Section 1033 implicitly includes a right for consumers to revoke their authorization to access their information. That section provides a right of access to data "upon request" of the consumer. 12 U.S.C. 5533(a). Once a consumer is no longer requesting the information, *i.e.*, once they revoke that request, any third party accessing the information based on the request no longer has permission to have such access.

The CFPB should require a mechanism to effectuate this revocation, because otherwise the right to revoke authorization will not be meaningful. Furthermore, consumers should be able to revoke the authorization either with the data provider or with the authorized third parties (*i.e.*, data aggregator or recipient). Both are important. The ability to revoke through the data provider is important because the consumer may not even be aware of who the data aggregator is or their existence. Conversely, the data aggregator may have access to multiple accounts, and it would be simpler for the consumer to see all of those access points and revoke access in one step.

Revocation will most likely be more important for ongoing uses than one-time uses. For one-time uses, the CFPB should not require consumers to revoke authorization; it should simply expire. For ongoing uses, the CFPB should consider requiring a simple, easy-to-use mechanism, such as a toggle switch. Many apps, especially mobile apps, feature toggle switches for consumers to grant or revoke permission. Many consumers are familiar with them and most can easily operate them.

Question 97 asks how the CFPB should address consumers' potential desire to revoke access for certain, but not all, use cases.

The CFPB should facilitate the ability of consumers to revoke ongoing access for some, but not all, use cases. Consumers should be able to do so either with the data provider, the data aggregator, or the data recipient. If a data recipient is using or a data aggregator is supplying the consumer's data for multiple uses, each use case should have its own authorization.

For ongoing uses and access, revocation should be made simple. Each authorization for a particular ongoing use should be displayed using a toggle switch which can be used to revoke authorization. For example, a company might seek authorization to access data for personal financial management, for processing payments on a platform, and for open-end credit account reviews. All of these authorizations, and the data recipient for those uses, should be shown on both the data provider's and

the aggregator's web/mobile app page and the consumer should be able to revoke authorization for each use by means of a toggle switch.

Question 117 asks for input on a proposed requirement for authorized third parties to periodically remind consumers how to revoke authorization. The CFPB is also considering requiring authorized third parties to provide consumers with a mechanism to request information about the extent and purposes of the authorized third party's access.

Both authorized third parties and data providers should be required to provide reminders about how consumers can view which third parties have access to the consumers' data and how to revoke these authorizations. For data providers, this could be as simple as email reminders or pop-ups on a mobile app every quarter: "you've permitted another company to have access to your account data, click here to see which companies and to turn off access."

4. Secondary Uses

The CFPB is considering proposals to limit a third party's use of information for purposes other than providing the product or service that the consumer requested, *i.e.*, secondary uses, by either the third party itself or downstream entities. The CFPB is considering prohibiting (1) all secondary uses; (2) certain high-risk secondary uses; (3) any secondary uses unless the consumer opts into those uses; and (4) any secondary use if the consumer opts out of those uses.

Question 98 and 99 ask for input on the above approaches and options

The CFPB should adopt a combination of options (2) and (3) above. It should prohibit high-risk secondary uses, such as debt collection or marketing of high-cost financial products (e.g., payday loans or fee-harvester credit cards), without the option of the consumer opting in for such uses. If that high-risk use is not the immediate purpose of the data access, the consumer is unlikely to understand or be in a position to meaningfully consent to that theoretical secondary use, and it could be portrayed in a misleading manner. Other uses should be prohibited unless the consumer opts in, such as pre-screening for mainstream credit products (*e.g.* general-purpose, not subprime, credit cards or qualified mortgages).[27]

Question 102 asks whether the CFPB should allow the secondary use of consumer-authorized information that has been de-identified.

We believe it is acceptable to use de-identified information for academic and research purposes. Such information must not include personal identifiers such as name or Social Security number. But researchers should be able to use alternative identifying numbers to track certain information (e.g., loan performance) for purposes of creating or adjusting underwriting models. In certain limited instances, the use of demographic data might be acceptable if used for a beneficial purpose, e.g., research on how to reduce racial disparities in underwriting models.

[27] For small dollar closed-end credit, a mainstream product would be defined as credit under 36% APR. A credit card would be considered mainstream if it was NOT required to make the disclosures required by Regulation Z, § 1026.60(b)(14).

The CFPB should investigate how to supply such de-identified information in a way that it cannot be re-identified. Data that can be re-identified should not be supplied in that form.

5. Retention

Question 103 asks for input on the CFPB's proposal to require authorized third parties to limit their retention of consumer-authorized information.

In general, we support limiting retention of consumer-authorized data to no more than what is necessary to provide the requested service or product, or for compliance with other laws. For lending purposes, this would generally mean retention by the recipient of not more than the two years required for compliance with Regulation B or Regulation Z. While it is important to limit the retention of information to protect consumer privacy and data security, the purpose of Regulation B in requiring records retention to prevent illegal discrimination is equally important. In addition, a longer time period may be required if the data holder is under investigation and has received a demand to retain records.

Question 109 asks what deletion requirements should be imposed on authorized third parties that utilize screen scraping, which collects more information than what is reasonably necessary to provide the product or service.

Data aggregators that utilize screen scraping should be required to immediately delete anything not necessarily for the use case before the data is shared with the data recipient. For example, if the recipient is using the information for credit underwriting based on a cashflow analysis, the aggregator should be required to delete information from credit card account data such as the identity of merchants and location of the transaction.

Question 110 asks whether the CFPB should allow authorized third parties to retain de-identified consumer information.

De-identified data can be retained for longer periods, so long as such data is not capable of being re-identified.

6. Data Security

The CFPB is contemplating two alternatives for data security requirements for authorized third parties. The first alternative would simply require third parties to comply with the FTC's Safeguards Rule or the banking regulators' Safeguards Guidelines. The second alternative would require third parties to develop, implement, and maintain a comprehensive written data security program appropriate to the third party's size and complexity, permitting the Safeguards Rule as an option for compliance.

Question 111 asks for input on these approaches

There are two critical issues with respect to data security:

- The CFPB should state that authorized third parties are subject to the FTC Safeguards Rule. In the SBREFA outline at page 45, the CFPB states that it "believes authorized third parties that seek to access consumer-authorized information are also likely subject to this [Safeguards] framework." We urge the CFPB to simply codify this statement in a rule, *i.e.*, explicitly state that

the FTC Safeguards Rule applies to authorized third parties, as well as data providers and data recipients to the extent they are not already explicitly covered by the banking regulators' Safeguards Guidelines.

- The CFPB should supervise larger participant aggregators in general, and specifically for data security. More importantly, we urge the CFPB to formally adopt a larger participant rule to supervise data aggregators and to examine them for data security as part of that supervision, using the same authority that the Bureau is currently exercising to examine the nationwide CRAs for data security. As noted above, supervision is especially important for those who access information about EBT cards, which are not protected against unauthorized use. Ensuring that the Safeguards Rule is actually being followed is just as critically important as the issue of coverage.

IX. Implementation Period

Questions 121 asks for input on an appropriate implementation period for complying with a final rule, other than the potential third-party access portal requirement.

We think that an implementation period of 180 days is more than sufficient. It has been over 10 years since statutory requirement in Section 1033 was enacted as part of the Dodd-Frank Act. During that time, there have been significant strides in the adoption and use of consumer-authorized data, despite the lack of a rule. Implementation of a final rule should be easier than normal because of the progress in technical advances and standard setting during this decade.

* * *

Thank you for the opportunity to submit these comments and the strong proposals under consideration as set forth in the SBREFA Outline. If you have questions about these comments, please contact Chi Chi Wu at cwu@nclc.org or 617-542-8010.

Respectfully submitted,

National Consumers Law Center
(on behalf of its low-income clients)

U.S. PIRG