December 28, 2023

Via regulations.gov
Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB–2023–0052/RIN 3170-AA78.

The National Consumer Law Center (on behalf of its low-income clients) (NCLC) is pleased to submit these comments in response to the Consumer Financial Protection Bureau (CFPB)'s Advanced Notice of Proposed Rulemaking regarding Consumer Access to Financial Records, Docket No. 2023-0052, issued October 31, 2023.[1] In general, we support the proposed regulation and believe it is a strong, protective rule that will ensure that consumers can share data from their deposit, prepaid, and credit card accounts without such access being misused or exploited. The consumer protections in the rule should serve as a model of how to safeguard consumer control and privacy when a consumer grants permission to a business to use data about themselves.

Even with this strong proposed rule, we do have some suggestions for improvement. The most critical of these suggestions are as follows:

- The CFPB should expand the scope of coverage of data providers to include payroll processors, debt collectors, closed-end creditors, and most especially, companies that process transactions for Electronic Benefits Transfer (EBT) recipients. (Section A)
- The CFPB should require data providers to (1) disclose in their consumer interfaces those third parties accessing the consumer's covered data and (2) provide a revocation mechanism for such access. (Section F)
- The CFPB should issue model forms for the authorization disclosure and data aggregator's certification, including mobile-friendly versions. The CFPB should also prescribe reading level and a timing requirement. (Section K.1)
- The consumer protections at proposed § 1033.421 are the most critical part of the proposed rule and we strongly support their adoption, including the prohibition against secondary uses of covered data. (Section L) Furthermore, the CFPB should limit each authorization disclosure to only one product or service. The CFPB should require a waiting period, such as 14 days, before a consumer can be solicited (which cannot be based on covered data) to consent to a second authorization disclosure for a second product or service. (Section L.3)

Additional suggestions are discussed throughout the text of these comments.

[1] The proposed rule is at 88 Fed. Reg. 74796 (Oct. 31, 2023). These comments were written by NCLC attorneys Chi Chi Wu and Carla Sanchez-Adams.

Table of Contents

A. Coverage of Data Providers (Proposed § 1033.111)

Proposed § 1033.111 specifies that the rule imposes duties on a data provider only with respect to two categories of financial products: Regulation E asset accounts and Regulation Z credit card accounts. However, the text of the statute at Section 1033 is not limited to deposit account and credit card data, but includes any "consumer financial product or service that the consumer obtained from such covered person." 12 U.S.C. § 5533.

Thus, we reiterate our call from our comments to the CFPB's Advanced Notice of Proposed Rulemaking (ANPR)[2] and our comments to the Outline of Proposals for the Small Business Review Panel (SBREFA Outline)[3] that there should be a broad scope of coverage for the Section 1033 rule. This scope should include payroll processors, debt collectors, closed-end creditors, and most important, EBT service providers. All of these entities are "covered persons" that provide a "consumer financial product or service" as discussed below and thus within the scope of the statutory text of Section 1033. Indeed, if Section 1033 is self-executing as some have argued, these entities already might be subject to its obligations.

While adding these data providers should not slow down the issuance of the final rule with respect to deposit and credit card accounts, we urge the CFPB to immediately start the process of issuing a new, second proposed rule to bring these covered persons within the scope of Section 1033.

1. Payroll processors

The CFPB should include payroll processor/data furnishers within the scope of data providers. These include companies that supply information to Equifax's The Work Number, such as ADP and Paychex. Since the Work Number is used for credit underwriting[4] and thus a covered person under 12 U.S.C. § 5481(6), furnishers of data to that CRA could be considered a "service provider," *id*. at § 5481(6)(B). In addition, payroll processors themselves should be considered covered persons because they provide "payments or other financial data processing products or services." *Id*. at § 5481(15)(A)(vii). Including payroll processors within the proposed rule would allow for competition by companies such as Pinwheel, Certree, and Argyle, so that the Work Number does not have a monopoly over this type of vital financial data.

2. Debt collectors

The CFPB should include debt collectors as covered data providers under the rule. Debt collectors are clearly covered persons, since collecting a debt related to a financial product or service is itself a

[2] Consumer Groups' Comments to the CFPB Regarding Consumer Access to Financial Records ANPR, February 4, 2021, https://www.nclc.org/wp-content/uploads/2022/08/Comments_CFPB_1033_ANPR-1.pdf.
[3] NCLC and USPIRG, Consumer Access to Financial Records, Small Business Regulatory Enforcement Fairness Act Review, Jan. 25, 2023, https://www.nclc.org/wp-content/uploads/2023/01/NCLC-Comments-to-CFPB-Section-1033-SBREFA-Outline.pdf.
[4] The Work Number, Instant Verification of Employment and Income for Mortgage, https://theworknumber.com/solutions/industries/mortgage-verification (visited December 28, 2023).

financial product or service under the Dodd-Frank Act, 12 U.S.C. § 5481(15)(A)(x). 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. Covering debt collectors under the Section 1033 rule 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.

3. Credit products other than credit cards

We reiterate our request from our SBREFA Outline comments that the rule should include closed-end credit products such as mortgages, auto loans, and installment loans. The text of Section 1033 includes any "consumer financial product or service," and all of these products qualify as such under 12 U.S.C. § 5481(15)(A)(i). Including access to data for closed-end products would be necessary for the creation of competitors to the nationwide consumer reporting agencies (CRAs).

4. EBT processors

Omitting EBT processors from the scope of a Section 1033 rule deprives a vulnerable low-income population of data access rights and protections that they need as much as, if not more, than consumers who have bank accounts and credit cards. Over 41 million people across the country rely on Supplemental Nutrition Assistance Program (SNAP) benefits, distributed and administered through EBT accounts, to feed their families and manage their household finances.[5]

EBT accountholders' ability to check their balance or review their transactions is severely limited by lack of Regulation E rights, portal outages, a lack of data made available to them within their portal, and slow responsiveness of existing portal infrastructure. Third parties offer accountholders alternative ways to access their EBT account balances and view their transaction histories; however, without coverage under the rule, EBT accountholders will not have the right to grant permission to these third parties.

NCLC has signed on to the letter from a coalition of advocacy groups organized by Prosperity Now and the Center for Law and Social Policy, and we direct the Bureau to this letter for additional information.

B. Compliance Dates (Proposed § 1033.121)

The CFPB has proposed the following dates for data providers to comply with the proposed rule's requirements to make covered data available (Proposed §§ 1033.201 and 1022.301):

> (a) Six months after publication of the final rule for: (1) depository institutions that hold at least $500 billion in total assets and (2) nondepository institution data providers that generate at least $10 billion in revenue per year.

[5] United States Department of Agriculture, Food and Nutrition Service, Supplemental Nutrition Assistance Program Participation and Costs, October 13, 2023, https://fns-prod.azureedge.us/sites/default/files/resource-files/snap-annualsummary-10.pdf.

(b) One year after publication of the final rule for: (1) depository institutions that hold between 50 billion and $500 billion in total assets; and (2) nondepository institutions that generate less than $10 billion in revenue per year.
(c) Two and a half years after publication of the final rule for depository institutions that hold between $850 million and $50 billion in total assets.
(d) Four years after publication of the final rule for depository institutions that hold less than $850 million in total assets.

We support these staggered compliance dates. Mostly importantly, we support the fact the proposed rule covers all data providers, even depository institutions with under $850 million in assets.

The CFPB has asked whether proposed rule should provide a grace period for depository institutions that do not have a consumer interface as of the effective date but subsequently offer such an interface to their customers. We believe that such a grace period is not necessary. Such a depository institution is likely to use a third party-core processor to establish its consumer interface, and such core processors should have the ability to offer a developer interface.

C. Standard Setting Bodies (Proposed § 1033.141)

The CFPB has proposed a scheme in which data providers must provide covered data using a "developer interface." This developer interface must provide data in a format set forth by a "qualified Industry standard," if one exists. In turn, a qualified industry standard is one that is established by a "fair, open, and inclusive standard-setting body." Such a standard-setting body must have attributes defined by proposed § 1033.141.

We support all of these concepts. We appreciate the requirement that a "fair, open, and inclusive" standard setting body must include consumer advocates, and more importantly, that consumer advocates must be included as part of the decision-making body. We also appreciate the requirement that the standard setting body must provide for due process and appeal rights

D. Covered Data (Proposed § 1033.211)

The CFPB has proposed defining the "covered data" that is required to be provided to include the following categories of information, as applicable:

- Transaction information, including historical transaction information of at least 24 months. This category includes amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges.
- Account balance.
- Information to initiate payment to or from a Regulation E account. This category includes a tokenized or non-tokenized account and routing number that can be used to initiate an Automated Clearing House transaction.
- Terms and conditions, including fee schedule, annual percentage rate or annual percentage yield, rewards program terms, any overdraft coverage opt-in, and whether a consumer has entered into an arbitration agreement.

- Upcoming bill information, including information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.
- Basic account verification information, limited to name, address, email address, and phone number associated with the account.

In general, we support this scope for what constitutes "covered data." We especially support the statement that a data provider would be deemed to make available sufficient historical transaction information if it makes available at least 24 months of such information. As the Bureau knows, Section 1033(c) states 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 conflicting with this section because 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.

As for additions to this list of information required to be disclosed as covered data, we recommend:

- For both deposit accounts and credit cards, require disclosure of any credit score or risk score used by the data provider, including scores issued by the nationwide CRAs, ChexSystems, or Early Warning Services.
- For deposit accounts, explicitly include "deposits" in Example 1 to paragraph (a).
- For deposit accounts, make clear that account balances include both available balance and actual balance.
- For deposit accounts, require disclosure of any criteria for account closure, at least to the consumer.
- For credit cards, require disclosure of both the required minimum payment for the billing cycle and the actual payment amount that the consumer paid for that cycle.
- For credit cards, require disclosure of the credit limit for the account.

The CFPB has asked for comment on tokenized account and routing numbers (TANs) in lieu of non-tokenized account and routing numbers, including whether TANs have any limitations that could interfere with beneficial consumer use cases. We do not support the sharing of TANs instead of non-tokenized numbers if that interferes with any common use cases for covered data, such as tax preparation (if account numbers are needed to ensure proper data matching) or check printing.

The CFPB also requested comment on whether data providers should also be required to make available information to initiate payments from a Regulation Z credit card. We would support such a requirement, if such information might be useful for consumers switching credit cards when the card number is stored with a merchant (e.g., Amazon) or digital wallet (e.g. Apple Pay), including for automatic payments.

E. Exceptions to Disclosure of Covered Data (Proposed § 1033.221)

The proposed rule has four categories of information that is not required to be disclosed:

1. Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors.

2. Any information collected for the sole purpose of preventing fraud or money laundering, or detecting other unlawful conduct. This does not include name and other basic account verification information, or information collected for another purpose.
3. Any information required to be kept confidential by another provision of law. However, these laws do not include privacy protections or other laws requiring protection of information for the benefit of the consumer.
4. Any information that the data provider cannot retrieve in the ordinary course of business.

With respect to the first exception, the proposed rule clarifies that it does not include Information that is merely an input to, or an output of, an algorithm, risk score, or predictor. The example given is an annual percentage rate, which is sometimes determined by an algorithm. We urge the CFPB to explicitly state, or give as an example, that the credit scores or other risks scores that are the ***product*** of a scoring algorithm are also not covered by this exception.

F. General Requirements for Data Provider and Consumer Interfaces (Proposed § 1033.301)

Proposed § 1033.301 sets forth the general requirement that data providers must establish and maintain both a developer interface and a consumer interface. Data providers must also provide covered data in the form of machine-readable files upon request.

Proposed § 1033.301(c) prohibits data providers from imposing any fees or charges on a consumer or authorized third party for making covered data available or responding to requests for data. Data providers also cannot charge for establishing and maintaining the interfaces required by this section. We strongly support this prohibition on fees and charges. It is critically important that data providers not impose barriers for consumers exercising their statutory right to access to covered data, whether through the developer interface or the consumer interface.

We also urge the CFPB to make clear that data providers cannot insist on any other consideration or quid quo pro for providing access to the required interfaces. For example, one major credit card issuer recently attempted to require that consumers consent to online-only delivery of billing statements if consumers wanted access to the issuer's consumer interface.[6] This practice should be prohibited under § 1033.301(c).

The CFPB has asked a whether there are other practices that the proposed rule should identify that might effectively make data unavailable to consumers and authorized third parties. As discussed below with respect to our comments on proposed § 1033.331(b)(1), a significant barrier to consumers' access to covered data about their accounts would be excessive requirements for consumer identification.

The CFPB notes that proposed § 1033.301 does not specify whether the requirements for a consumer interface need to be satisfied by a mobile application interface or an online banking portal "as long as collectively the two applications satisfy the requirements." The CFPB has also asked to what extent do

[6] Miriam Cross, Phasing out paper statements? Citi's stumble holds lessons for others, American Banker, Nov. 13, 2023, https://www.americanbanker.com/news/phasing-out-paper-statements-citis-stumble-holds-lessons-for-others.

data providers currently inform consumers using mobile banking applications that additional information may be available through the desktop version of online banking interfaces. We have not observed data providers providing such information. We urge the CFPB to mandate that data providers provide the same information in a mobile application as a desktop consumer interface. If information is too dense or voluminous to provide on the main screen of a mobile application, it can be provided secondarily through the use of hyperlinks or pop-ups. Given that many low- and moderate-income consumers only have a mobile phone for Internet access, ensuring device informational parity is both critical and is possible using the navigational capabilities of the mobile format.

Finally, we urge that proposed § 1033.31 include an additional requirement: that the consumer interface include information as to which third parties are accessing the consumer's covered data, so that consumers are aware of when their covered data is being shared. This is important so that consumers are always aware of which third parties they have shared their data with, and don't risk forgetting. More critically, such information plus the ability to revoke authorization as discussed in Section I.2 will allow the consumer to take immediate action if the consumer didn't actually authorize the third party to have access, but the access is the result of error or fraud.

G. Requirements for Developer Interfaces (Proposed § 1033.311)

Proposed § 1033.311 sets forth a number of requirements for a developer interface. These include:

> 1. The developer interface must make available covered data in a standardized format. This format must be set forth in a qualified industry standard. If none exists, the format used by the interface must be one that is widely used by the interfaces of similarly situated data providers. (Proposed 1033.311(b))
> 2. The developer interface must meet certain performance specifications, including a rate of response to requests of at least 99.5%, with responses made within 3.5 seconds. (Proposed 1033.311(c)(1))
> 3. A data provider cannot unreasonably restrict the frequency to which it responds to requests for covered data, *i.e.*, it cannot impose access caps on the developer interface, except under specific limited circumstances. (Proposed 1033.311(c)(1))
> 4. The developer interface must not permit a third party to access information using the consumer's credentials for the consumer interface, *i.e.*, screen scraping (proposed 1033.311(d))
> 5. Data providers must abide by the data security requirements of the Gramm-Leach-Bliley data security rule applicable to them, *i.e.*, the banking regulators' rules for depository institutions and the FTC Safeguards Rule for other data providers.

We support all of the above requirements, especially the performance specifications and data security requirements for non-depository institutions. The CFPB has asked a number of questions about these requirements. We provide answers to the following:

> i. The CPFB asks whether the option to use a format that is widely used by the interfaces of similarly situated data providers in proposed § 1033.311(b)(2) should also be available if there is a qualified industry standard. We do not think the option in proposed § 1033.311(b)(2) should apply if there is a qualified industry standard. Indeed, once a qualified industry standard is developed and available, this paragraph should be removed and all data providers should be required to use a qualified industry standard.

ii. The CFPB has asked whether it should define the word "format" and whether this definition should mean specifications for data fields, status codes, communication protocols, or other elements to ensure that third party systems can communicate with the developer interface. We would support a definition of "format" that would result in not only a common industry standard, but a standard that includes specifications for status codes, data fields, and the like. The more steps that the CFPB can take to ensure that there is a common language use by data providers, third parties, and data aggregators when transmitting and access covered data, the better. More standardization ensures that there is more of a common understanding and less of a possibility of misunderstanding. While there are many problems with the nationwide CRAs, the presence of the Metro 2 reporting format as a common format and data dictionary is helpful to ensure a common language in credit reporting.

iii. The CFPB asks whether it should allow for a later compliance date for the requirement in 1033.311(b) that data providers make covered data available in a standardized format. We do not think the CFPB should provide for a later compliance date. There are already formats that are widely used by the developer interfaces of data providers, such as FDX.

iv. The CFPB asks whether the final rule should include a presumption that access caps are unreasonable unless undertaken for a period only as long as necessary to ensure that a third party request does not interfere with the receipt of and response to requests from other third parties accessing the interface. We agree that such a presumption would be a useful, bright line rule as to when an access cap or denial based on frequency of access is unreasonable, and would support the CFPB establishing it.

H. Denials of Access to Covered Data (Proposed § 1033.321)

Proposed 1033.321 sets forth the circumstances in which a data provider can deny access to covered data based on risk management concerns. The CFPB has asked whether the Bureau should specify types of evidence that a third party would need to present about its data security practices that would give a data provider a reasonable basis to grant or deny access based on risk management concerns. We believe that such guidance would be helpful in establishing the "rules of the road" for denials of access based on data security issues. In general, denials of access to covered data based on risk management concerns should only be allowed in narrow circumstances.

The CFPB has also asked for comment about the idea of having an independent accreditation or credentialing system for third parties. We would support such an idea. There should be a list of credentialed third parties maintained by an independent body, perhaps one or more of the "fair, open, and inclusive standard-setting bodies." And if there is a denial of access for a third party based on data security issues, that third party should be able to petition the standard-setting body for inclusion on the list of acceptable entities to grant access.

The CFPB has also asked whether it should require third parties to submit to the Bureau a link to the website on which its identifying information required by proposed 1033.321(d)(2) is disclosed. This would enable the CFPB to publish a directory of links that data providers and other members of the public could use. But such a directory would not serve as a list of credentialed or approved third parties,

since a data provider could still deny access to these third parties based on other concerns, such as data security practices. Such a directory could cause confusion if a consumer tried to authorize access for a third party listed in the directory, and the data provider denied access. Therefore, if there is to be a directory, it should only include approved or credentialed third parties.

CFPB also seeks comment on whether data providers should have to provide information or notice to the CFPB regarding their procedures and decisions to approve or deny third parties for access to their developer interfaces. We support such reporting requirements.

I. Responses to Requests for Covered Data (Proposed § 1033.331)

Proposed § 1033.331 governs the responses that data providers must provide when a consumer or a third party makes a request for covered data. For consumers, the data provider must:

(1) authenticate the consumer's identity; and
(2) identify the scope of the data requested.

For third parties, the provider must also conduct tasks (1) and (2), plus it must

(3) authenticate the third party's identity; and
(4) confirm that the third party has followed the authorization procedures in § 1033.401.

This section also lists the bases on which the data provider is can decline a request for covered data, such as the application of an exception under § 1033.221, risk management concerns under § 1033.321, or the expiration or the consumer's revocation of their authorization under § 1033.421(b)(2).

1. Limitations on requests for identity authentication (Proposed § 1033.331(a)(1) and (b)(1)(i))

The CFPB should include a statement in the proposed rule that the data provider cannot make unreasonable or excessive demands when seeking to authenticate the identity of the consumer. As we noted in our comments to the SBREFA Outline and our May 2022 comments to the CFPB regarding its proposed rule to protect trafficking survivors,[7] we have seen such excessive requirements by the nationwide CRAs, such as:

> i. Requiring consumers to answer a series of questions based on information in the consumer's file or account, which often are too difficult for consumers to answer, tripping them up.
> ii. Requiring the consumer to provide documentation such as a copy of a driver's license or state ID, utility bill, and bank or insurance statement, but then rejecting these documents for the flimsiest of reasons such as a small discrepancy in the consumer's address (no unit number).

We do not want consumers to face similar barriers in accessing information under Section 1033. The CFPB has noted that in today's market, authentication typically consists of a provider asking the consumer to supply their account credentials. 88 Fed. Reg. at 74823. However, there is nothing in the text of Proposed § 1033.331 that limits authentication to account credentials or another type of easily

[7] 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.

supplied authentication (e.g., verification using a code via by SMS code or email). The CFPB could provide these as examples of identity authentication. At a minimum, the rule should prohibit excessive or unreasonable demands for identity authentication.

2. Provider confirmation of third party request for covered data (Proposed 1033.331(b)(2))

When a third party is requesting the data, proposed 1033.331(b)(2) ***permits*** the provider to ask the consumer to confirm the relevant accounts and scope of data. We urge that the rule ***require*** that the provider send a confirmation to the consumer when it receives a third party request for information. This will ensure 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. We note that the CFPB states it "has preliminarily determined that data providers should confirm the third party's authorization with the consumer." 88 Fed. Reg. at 74,823. However, the actual language of the regulation is permissive rather than mandatory.

3. Joint account holders and authorized user accounts (Proposed 1033.331(d))

Proposed § 1033.331(d) provides that if the data provider receives a request for covered data from one accountholder for a jointly held account or an authorized user of that account, the provider must make the covered data available subject to the other requirements of rule. The CFPB has asked whether the other accountholders should receive notice or have an opportunity to prevent access after such notice.

We support allowing each joint account holder to make request for covered data, since each account holder may have separate needs for the information. The non-requesting joint account holder should receive a notice, unless the requesting consumer actively indicates that such a notice would be harmful to the consumer because it poses a risk to their safety (e.g., they are a domestic violence survivor and the joint account holder is their abuser). The other account holder should not be permitted to prevent access to the covered data.

The CFPB also asks whether authorized users should have a right to access covered data about an account. We believe the right for an authorized user to access covered data for an entire account should be limited to spouses. In all other cases, only the covered data regarding the authorized user's own transactions should be accessible if such transactions are segregated (as the case with most credit cards today, when the authorized user has their own card number). In non-spousal cases, an authorized user is not liable on the account, except possibly for their own transactions.

Access to the entire account for authorized user spouses would support the goal of Regulation B's provision on spousal credit reporting, which implements the goals of the Equal Credit Opportunity Act to ensure that married women benefitted from the credit history of credit card accounts held in their husband's name. Reg. B, 12 C.F.R. § 1002.10. In non-spousal cases, the authorized user may be a child or relative who should not have access to the parent or primary accountholder's transactions.

4. Provider-located mechanism to revoke authorization to access covered data (Proposed 1033.331(e))

Proposed § 1033.331(e) permits, but does not require, that a data provider provide a mechanism for the consumer to revoke their authorization for a third party to access covered data. We recommend that data providers be *required* to offer such a mechanism of revocation. We recognize that the CFPB stated that it did not propose such a requirement because of the burden on smaller providers. 88 Fed. Reg. at 74,824. However, such a revocation mechanism will likely be built into the developer interfaces suppled by core processors or other third parties.

Requiring the provider to supply a revocation mechanism will reduce the amount of friction that consumers experience when they observe from the provider's consumer interface that a third party is accessing their data, perhaps something the consumer had forgotten about, and the consumer wishes to revoke that authorization. Of course, this means that the CFPB should also require providers to display information on which third parties are accessing covered data in their consumer interfaces, as discussed in Section F.

Requiring the provider to supply a revocation mechanism is also critical in cases where access to covered data is due to error, fraud, or identity theft. In such cases, the consumer might not know how to reach the third party. Or the third party might require the consumer to produce a password that the ID thief created or use a mobile number/email address for verification that is in the control of the thief.

Finally, if a consumer suspects that the third party to which they gave access is abusing the data or engaged in a questionable practice, they should be able to revoke authorization immediately. Being able to this through the data provider's website is much safer and surer than doing it through the third party. If the third party is engaged in questionable practices or undergoes some sort of turmoil (e.g., bankruptcy), revoking through the third party may be slow or it may become unresponsive.

J. Data Provider Policies and Procedures (Proposed § 1033.351)

Proposed § 1033.351 sets forth requirements for data providers to have policies and procedures covering various issues, including policies and procedures reasonably designed to:

- Achieve the objectives set forth in the requirements for data providers in the proposed rule;
- Create a record of when it makes covered data available, as well as what data fields are not made available pursuant to an exception in proposed § 1033.221;
- Create a record of when the provider denies a third party or a consumer's request for access to covered data under § 1033.321 (risk management concerns) or § 1033.331 (identity authentication, revocation or expiration of authorization), including the basis for the denial. The reasons for the denial must be communicated to the third party;
- Ensure that covered data is accurately made available through the developer interface; and
- Ensure retention of records that are evidence of compliance by the data provider with the proposed rule.

In general, we support the proposed requirements for policies and procedures on the part of the data provider. We especially appreciate the requirement for communications for a denial of access, including the reasons for such denial, which is something that we supported in our comments to the SBREFA

Outline. We suggest the CFPB to also require the provider to explain what actions or steps a consumer or third party must take to address the denial.

We appreciate the requirement in proposed § 1033.351(c)(1) for the provider to maintain policies and procedures regarding accuracy. The CFPB notes that it "has preliminarily determined that a data provider's policies and procedures should focus on the accuracy of transmission rather than the underlying accuracy of the information in the data provider's systems." 88 Fed. Reg. at 74,828. One reason given for this is that covered data "is likely subject to several legal requirements regarding accuracy. For example, Regulation E protects consumers against errors, and Regulation Z protects consumers against billing errors." *Id.*

While the accuracy of transmission is certainly critical, it may not be entirely sufficient to rely on the Regulation E and Regulation Z dispute rights to ensure accuracy in the underlying covered data. Both regulatory regimes have strict time limits for exercise of those rights. For example, Regulation Z and the Fair Credit Billing Act (FCBA) require a billing error dispute to be sent in writing within 60 days of the periodic statement containing the error. 15 U.S.C. § 1666(a). Regulation E and the Electronic Funds Transfer Act (EFTA) have a similar timeframe. Thus, if the underlying covered data is inaccurate but past these timeframes, the consumer has no right to correct the error under FCBA or EFTA. Such instances may occur when an error might not have a monetary impact but could have an informational one.

For example, a consumer simply may have not noticed that payment to a credit card was credited 2 weeks late instead of 2 days late. For purposes of paying a late fee, this time difference does not matter, but it could matter for other credit underwriting. The merchant for a debit card or ACH transaction could be misidentified, which might matter for tax preparation reasons. For example, a $100 donation to a charitable organization (ACLU Foundation) might be misidentified as going to its non-501(c)(3) counterpart (ACLU). A consumer might not think to correct this because the amount is the same, until they notice it when preparing their tax return.

We urge the CFPB to give consumers the ability to dispute an error in the underlying covered data, similar to the consumer's right to dispute errors on their credit report with a data furnisher under the Fair Credit Reporting Act, 15 U.S.C. § 1681s-2(a)(8). We suggest that the CFPB modify the requirement at proposed 1033.351(c)(2)(ii) that a data provider should have policies to "address information provided by a consumer or third regarding inaccuracies" to instead require that the data provider conduct a "reasonable investigation" of inaccuracies that a consumer has brought to the provider's attention, and should cover inaccuracies both in transmission and in the underlying data.

K. Authorizations for Data Access by Third Parties (Proposed §§ 1033.401 and 1033.411)

Proposed § 1033.401 sets forth the requirements for a third party to have access to covered data on behalf of a consumer. The third party must be using the covered data to provide a product or service requested by the consumer and must also:

> (a) provide an authorization disclosure;
> (b) provide a certification that the third party will comply with the consumer protections in proposed § 1033.421; and

(c) obtain the consumer's express informed consent for the third party to access the covered data by obtaining the consumers written or electronic signature on an authorization disclosure.

Proposed § 1033.411 sets forth the requirements for the authorization disclosure. This disclosure must be clear, conspicuous and segregated from other material. It must contain

(1) the name of the third party, i.e., the user of the covered data;
(2) the name of the data provider, i.e., the depository institution or card issuer;
(3) a brief description of the product or service that the third party will provide, and a statement that the covered data will be used only to provide that service or product;
(4) the categories of covered data that will be accessed;
(5) the certification that the third party will comply with the consumer protections in proposed § 1033.421; and
(6) a description of how the consumer can revoke their authorization.

1. Formatting and timing

The CFPB has also asked for comment on whether the Bureau should establish additional or more prescriptive requirements, such as:

- a word count or reading level
- a timing requirement, such as a requirement that the authorization disclosure be provided close in time to when the third party would need consumer data to provide the product or service
- a prescribed format or sample form that is set forth in a qualified industry standard.

We strongly urge the CFPB to adopt all of these requirements. A word count and reading level is necessary to ensure that the authorization disclosure is comprehensible to most consumers. We suggest requiring the use of language at a sixth grade level. A model form is crucial to ensure that the disclosure is understandable and salient, and has a chance of actually being read. There is certainly precedent for a model forms, model language, reading level requirements and more, such as credit card account opening disclosures under Regulation Z, mortgage forms under Regulation X, and privacy notices under Regulation P.

As for timing, the CFPB needs to ensure that authorization disclosures are not provided too far in advance, as that uncouples the authorization disclosure from the actual access. It creates the risk that the consumer will forget that they had granted authorization in the first place. We suggest that the disclosure be given no earlier than 14 days prior to when the third party starts providing the service or product.

The CFPB should also develop model interfaces, such as using 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 rule should require that disclosures be mobile friendly when made on a mobile phone.[8] Many low-and moderate-income consumers – indeed, many consumers generally – now primarily rely on their mobile phones to view disclosures and

[8] *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).

websites. That is another reason to mandate the use of toggle slides and not click-throughs from a pop-up screen.

2. Joint account holders

The CPFB has asked whether, for a joint account, the other account holder(s) should receive notification or a copy of the authorization disclosure or should have an opportunity to object. We believe that the other account holders should receive notice, unless the consumer actively indicates such notice would be harmful to the consumer because it poses a risk to their safety (*e.g.*, they are a domestic violence survivor and the joint account holder is their abuser). We do not think the other account holders should be given the right to object.

3. Language and disability access

Proposed § 1033.411(c) requires the authorization disclosure to be in the same language as the one used by the third party to "convey the authorization disclosure" to the consumer. This latter phrase appears to be a bit ambiguous – does it simply mean the language used in sending or displaying the disclosure to the consumer? Or is it the language in which the third party asks the consumer to sign the disclosure? One can imagine a situation in which all of the marketing and solicitation is conducted in one language, but the actual hyperlink to the webpage displaying the authorization disclosure – the "conveying" of the disclosure – is in English. We suggest that proposed § 1033.411(c) instead require a translation into any language used to solicit the consumer to give consent to the third party to access the data, or used to solicit the consumer to purchase or use the product or service for which the covered data will be used.

The CFPB asks whether the rule should contain requirements relating to the accessibility of the authorization disclosure for disabled persons, noting that it has "preliminarily determined that the Americans with Disabilities Act (ADA) and its implementing regulations would already require that the authorization disclosure be provided in an accessible format." 88 Fed. Reg. at 74,831. We urge the CFPB to include an accessibility requirement in the rule, to prevent any ambiguity in case there is disagreement about the applicability of the ADA.

4. Additional content and protections

The CFPB has also asked whether the authorization disclosure should include additional content such as the names of other third parties with whom data may be shared, the third party's contact information, or how frequently data will be collected. We support such information being disclosed, especially the identity of other third parties, which is very important for the consumer to know. To avoid the authorization being too cluttered, certain information such as contact info could be included on separate webpages via hyperlinks in electronic disclosures.

We also urge that the authorization disclosures include information about the alternatives if the consumer does not consent. 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." 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)."

The CFPB has asked whether the rule should include additional consumer protections, such as express prohibitions on false or misleading representations or omissions to induce the consumer to provide consent to the third party's access to covered data. While false or misleading representations would violate several other statutory prohibitions, including Section 1031 of the CFPA and Section 5 of the FTC Act, adding such a prohibition to the Section 1033 rule could be useful.

5. Exceptions

The CFPB has asked whether there are third parties for which the above requirements would not be appropriate, particularly smaller or non-commercial parties. We cannot think of any such third parties in terms of commercial users - in such cases, the consumer is always the smallest and most vulnerable entity. Another reason for the CFPB to provide a model authorization disclosure is for the benefit of small commercial parties to have an "off-the-shelf" disclosure that they can use.

For non-commercial users, there may need to be provisions for access to covered data in the consumer interface by an individual or natural person in certain circumstances. This would include a family member who is an executor of an estate or the guardian of a minor or incapacitated consumer.

L. Consumer Protections (Proposed § 1033.421)

1. General

Proposed § 1033.421 sets forth the obligations of third parties who access covered data with the consumer's authorization. This section contains the critical consumer protections to ensure that the access to covered data benefits the consumer and is used solely for the product or service that the consumer requested. It is **THE** most important section in the proposed rule. We are pleased to see that the CFPB has issued strong, robust consumer protections for third party access to data. We wholeheartedly support this section of the rule and believe it is a model for privacy protections for data access. We believe these protections are necessary to carry out the objectives of Section 1033.

2. Scope of collection, use, and retention. (Proposed § 1033.421(a)(1) and (b)(1)).

Proposed § 1033.421(a)(1) limits the collection, use, and retention of covered data to "what is reasonably necessary to provide the consumer's requested product or service." We are pleased to see this limitation of collection to what is reasonably necessary, which is essentially a data minimization standard, *i.e.*, the collection of data should be minimized to only that which is needed for the product or services. Thus, for example, if the requested service is bill payment, then the third party payment processor should only collect from a data provider bank the amount of information necessary to make the payment, *i.e.*, available balance and tokenized/non-tokenized account and routing number. There is no need for information about other individual transactions in the bank account and thus that data should not be collected.

We also support proposed § 1033.421(b)(1), which provides that the limitations on collection of covered data include not only the scope of the data collected, but the duration and frequency of collection. Thus, for example, if the third party only requires access to covered data for a one-time use, such as underwriting a closed-end loan, it should not be permitted to continue accessing the covered data after the loan has been approved and disbursed.

3. Limitations on secondary uses (Proposed § 1033.421(a)(1) and (2))

The limitation on the use of covered data to what is reasonably necessary to provide the requested product or service essentially establishes a prohibition on secondary uses. In addition, proposed § 1033.421(a)(2) contains a bright-line prohibition against certain secondary uses of covered data, namely targeted advertising, cross-selling of other products or services, and sale of the covered data. We strongly support these provisions and urge the CFPB not to weaken them. These protections are vital to ensure that access to covered data benefits consumers and does not harm them.

We note that these protections are stronger than those contained in other privacy regimes, most particularly the Gramm-Leach-Bliley Act (GLBA). Some stakeholders have cited this as a problem with the proposed consumer protections in proposed § 1033.421. However, the fundamental problem presented by this disparity lies in the fact that GLBA is such a weak privacy regime and needs to be strengthened. The fact that GLBA is so weak is not a reason to make the consumer protections equally weak in the Section 1033 rule.

The proposed protections in § 1033.421 are especially important given that some of the third parties that use covered data are notorious for cross-marketing based on questionable access to sensitive data. For example, one sector that accesses and uses covered data is tax preparation software providers, which may access the data to help consumers prepare an IRS Schedule B or D. An investigation by the news outlet the Markup found that tax preparation companies H&R Block, TaxAct, and TaxSlayer were transmitting sensitive financial information to Facebook when consumers filed their taxes online, including data on consumers' income, tax filing status, refund amounts, and dependents' college scholarship amounts.[9] The CFPB must prohibit any similar misconduct in the use of covered data accessed pursuant to Section 1033.

We note that the prohibition on secondary uses of covered data would not prohibit the third party from marketing or soliciting the consumer for additional products or services based on information other than covered data, *e.g.*, the third party would still be able to cross-market products or services to the consumer simply based on having the consumer's email address or the fact that the consumer is a current customer. This type of cross-marketing should also be subject to protections because of the potential for confusion or abuse if it involves a solicitation by the third party to access covered data for the second product or service.

We are concerned that a third party might include both the consumer's requested use and a second use in a single authorization disclosure, or seek consent to two authorization disclosures presented in close sequence in a way that may confuse consumers. We urge the CFPB to adopt provisions that would de-

[9] Simon Fondrie-Teitler, Angie Waller, and Colin Lecher, Tax Filing Websites Have Been Sending Users' Financial Information to Facebook, Nov. 22, 2022, https://themarkup.org/pixel-hunt/2022/11/22/tax-filing-websites-have-been-sending-users-financial-information-to-facebook.

couple any solicitation for a consent to use covered data for a second product or service. First, the CFPB should explicitly state that each authorization disclosure can only involve one product or service that is requested by the consumer. Second, we suggest the CFPB require a waiting period, such as 14 days, before a consumer could be solicited to consent to a second authorization disclosure after the first one. Such a waiting period has a precedent in the prepaid card rule, which requires the issuer to wait 30 days before adding a credit feature to a prepaid card. 12 C.F.R. § 1026.61(c)(1).[10]

Finally, we urge the CFPB to prohibit the solicitation of a second authorization disclosure for certain uses for covered data. These would include debt collection, marketing for harmful high-cost credit products (e.g., payday loans or fee-harvester credit cards), employment, and law enforcement (without a subpoena).

4. One-year maximum duration of authorization (Proposed § 1033.421(b)(2)-(4))

Proposed § 1033.421(b)(2) sets out a one-year limit as the maximum duration for an authorization to access covered data. In order to collect covered data beyond one year, proposed § 1033.421(b)(3) requires a third party to obtain a new authorization. Once an authorization expires, the third party must not only stop accessing the covered data; it cannot retain the data that it already collected unless it is necessary to provide the requested service or product.

We strongly support all of these provisions. A firm maximum duration of one year balances the need to protect the consumer from having their covered data collected beyond that time frame that is necessary, while avoiding a need for frequent re-authorizations for ongoing uses such as payment processing.

The CFPB has asked for comment on the alternative of using a maximum period based on dormancy, *i.e.*, a third party would be required to stop collecting data only after a period of non-use by a consumer. We do not favor a dormancy-based standard because it could create ambiguity and confusion. It could be difficult in some instances to determine at what point a consumer stopped using a product or service, and thus when the third party would be required to stop collecting the covered data.

5. Exceptions to ban on secondary use (Proposed § 1033.421 (c))

Proposed § 1033.421(c)(1)(and (2) allows certain uses of covered data even if the use is not directly for the purpose of providing the requested product or service. These are essentially an exception to the prohibition on secondary uses and allow:

(1) uses required by law, including to comply with a subpoena or summons; and
(2) uses to prevent potential fraud

[10] We recognize that a federal District Court struck down this 30-day waiting period in PayPal, Inc. v. Consumer Fin. Prot. Bureau, 512 F. Supp. 3d 1 (D.D.C. 2020). Unfortunately, this part of the decision was not raised in the appeal that led to the D.C. Court of Appeal's decision at 58 F.4th 1273. We do not understand why this issue was not appealed, given that the District Court's decision was based on a frankly illogical reason – that "the Bureau's authority under TILA is limited to disclosure of credit terms and does not extend to regulation of a consumer's access to or use of credit." 512 F. Supp. 3d at 11. The idea that the CFPB can only adopt disclosure rules under TILA is obviously very wrong given that TILA includes numerous substantive provisions governing the use and access to credit, including the entire Credit CARD Act of 2009.

The CFPB has requested feedback on whether the rule should permit third parties use or to solicit a consumer's opt-in consent to engage in secondary uses with de-identified data. We believe it should be permissible for a third party to engage in research or study using de-identified data. Data used for research 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.

However, we oppose any use of de-identified or anonymized data for the purposes of marketing or any purpose other than research. We have seen examples of supposedly de-identified data used for marketing by the nationwide CRAs, as described in our comments to the CFPB's Request for Information on Data Broker Practices.[11] We do not want de-identified covered data used for such purposes.

6. Accuracy

Proposed § 1033.421(d) requires the third parties to maintain written policies that are reasonably designed to ensure that covered data is accurately received from a data provider and accurately provided to another third party. In developing these policies, the third party must consider (1) accepting data in a standard format that is either set forth in a qualified industry standard or is widely used by data providers under § 1033.311(b); and (2) addressing inaccuracies in the covered data when brought to its attention.

As with data providers discussed at Section J above, we urge the CFPB to give consumers a stronger right to dispute an error in the underlying covered data, similar to the consumer's right to dispute errors on their credit report, by requiring the third party to conduct a "reasonable investigation" of inaccuracies that a consumer or other third party has disputed. In addition, we urge the CFPB to impose accuracy requirements on data aggregators in proposed § 1033.431.

7. Data security requirements (Proposed § 1033.421(e))

In collecting and using covered data, proposed § 1033.421(e) requires that a third party must comply with the requirements of the GBLA data security rule applicable to them, *i.e.*, the banking regulators' rules for depository institutions and the FTC Safeguards Rule for other data providers. We support this requirement.

8. Ensuring compliance by other third parties (Proposed § 1033.421(g))

If the third party will be sharing covered data with another third party, proposed § 1033.431(f) requires the first third party to ensure that there is a provision in the contract with the second third party that the latter will comply with the provisions of § 1033.421. We support this provision and believe it is necessary to prevent downstream users of covered data from misusing or exploiting the data. We note

[11] NCLC Comments to CFPB RFI on Data Brokers, July 14, 2023, https://www.nclc.org/resources/comments-to-cfpb-rfi-on-data-brokers/.

that under § 1033.421(a), the sharing of covered data should be permissible only when it is necessary in order for the first third party to provide the requested product or service.

9. Required informational disclosures (Proposed § 1033.421(g))

Proposed § 1033.421(g) requires the third party to provide the following:

> (1) A copy of the signed authorization disclosure.
> (2) Contact information where consumers can ask questions about the third party's access to covered data.
> (3) Upon request, the following: categories of covered data collected, reasons for collection, names of parties with whom covered data was shared and reasons for sharing.

We support the requirement for the third party to provide all of this information.

10. Revocation of authorization (Proposed § 1033.421(h))

Proposed § 1033.421 (h) requires the third party to provide a means to revoke an authorization. The revocation should be as easy to access as the initial authorization, and should not be subject to any costs or penalties. After a consumer revokes their authorization, the third party must stop collecting covered data and cannot use or retain the data unless it is necessary to provide the consumer's requested product or service.

We strongly support all of these provisions, especially the prohibition against imposing any costs or penalties for revocation. This prohibition against imposing any penalties should presumably prevent the third party from taking any retaliatory measures against the consumer. For one thing, the CFPB has stated that this provision allows the consumer to allow access to covered data for one purpose (e.g. tax preparation) but revoke it for another (e.g., payment app). 88 Fed. Reg. at 74,840. The prohibition against any penalties should also prevent a third party from treating the consumer worse than other consumers who have not granted access. For example, if a consumer revokes access to covered data at a payment app but the app offers a version without covered data access, such as the case with Venmo, then the app cannot deny the consumer access to the latter.

The CFPB has asked whether, following revocation, additional protections for consumers or flexibilities for third parties are warranted. We support limiting the retention or use of covered data only for the purpose of providing the requested product or service. Even in that circumstance, the consumer should be notified that the data will be retained for that purpose. It would be appropriate, however, to make an exception to this rule for the retention and use of anonymized, de-identified data for research, including fraud prevention research.

Finally, the CFPB should make explicit that the right to revoke an authorization is non-waivable.

M. Role of a data aggregator (Proposed § 1033.431)

Proposed § 1033.431 sets forth the requirements when a data aggregator is involved in accessing covered data. It allows the data aggregator to obtain the authorization from the consumer, although

the third party is ultimately responsible for compliance with the authorization requirements of § 1033.401. The aggregator must also agree to comply with the consumer protection requirements in § 1033.421, except for the disclosures required by subsection (g). The name of the aggregator and a brief description of its services must be included in the authorization disclosure. We support the requirements that the data aggregator must certify its compliance with § 1033.421 and that the authorization disclosure must include information regarding the aggregator.

The CFPB has asked whether it should impose formatting or language access requirements for an aggregator certification. We support such requirements. The certification should be in any language that the authorization disclosure was required to be provided in, as discussed in Section K.3 of these comments. Also, as we suggest with the authorization disclosure in Section K.1, we believe the CFPB should issue a model form and requirements with respect to reading level.

N. Record retention (Proposed § 1033.441)

Proposed § 1033.441 sets forth record retention requirements for third parties that are covered persons. It requires such covered persons to retain records of compliance with the rule for three years after the consumer's most recent authorization, including the authorization itself and any certification from a data aggregator. We support this record retention requirement.

O. Adding the provision of financial data processing products or services to the definition of "financial product or service" (proposed § 1001.2(b))

The CFPB has proposed adding a new provision to part 1001. Proposed § 1001.2(b) would include in the coverage of "financial product or service" the following: providing financial data processing products or services by any technological means, including processing, storing, aggregating, or transmitting financial or banking data, alone or in connection with another product or service.

We urge the CFPB to use language to ensure that this provision does not undermine the Fair Credit Reporting Act (FCRA) coverage of data aggregators that provide such products and services. We are concerned that some aggregators might argue that if their services are covered under § 1001.2(b), then they are a type of entity that is not a "consumer reporting agency" under the FCRA. For instance, a recent court decision held that a company was not a CRA under the FCRA because it was instead a "data broker." Cooper v. Milliman, Inc., 2023 WL 8112049 (W.D. Wash. Nov. 22, 2023). The court failed entirely to realize that an entity can be both a CRA and a data broker – that CRAs are actually a subset of data brokers.

We appreciate the statement in the Supplementary Information, 88 Fed. Reg. at 74,801, that a data aggregator is a CRA if the covered data bears on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living and is used or expected to be used, or collected, for "permissible purposes" as defined by the FCRA, such as when a third party uses the data to underwrite a loan to a consumer, and when the entity, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating such data for the purpose of furnishing reports containing the data to third parties. However, we urge the CFPB to include something in § 1001.2(b) itself regarding this issue, such

as a proviso at the end that "Such person may also be a consumer reporting agency under the Fair Credit Reporting Act."

* * *

Thank you for the opportunity to submit these comments and for the strong proposals under consideration as set forth in the NPRM. 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)