National Consumer Law Center
Fighting Together for Economic Justice

NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

February 12, 2020

Via email
Kathleen Kraninger
Director
Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, DC 20552

Re: Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act

Dear Director Kraninger:

Thank you for inviting me to speak at the Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act. I am pleased to submit the following statement, along with the attached two documents, on behalf of our low income clients in response to your request for written statements for this Symposium.

Over the past few years, there has been a rapidly growing use of data aggregators to access consumers' bank account transaction and other account data in connection with a variety of financial products and services. Use of this data can be beneficial for consumers, but it also poses risks. The CFPB should work to ensure safe use of consumers' data.

I. The Benefits and Risks of Bank Account Transaction Data Aggregation

Access to consumers' account data has the potential to enable many products and services that may be beneficial to consumers, including use of cash flow data to improve access to affordable forms of credit, products that encourage savings, and a variety of services that help consumers better manage their finances.

While financial institutions have legitimate security concerns about how their customers' data is accessed, they should not block access to that data for the purpose of stifling competition. To that end, we appreciate that the Bureau listed "Access" as a key principle in its 2017 *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation.* As the CFPB stated, "Access" includes the ability for "[c]onsumers [to be] able, upon request, to obtain information about their ownership or use of a financial product or service from their

product or service provider". We believe that this principle should be part of any regulatory issuance by the Bureau to implement Section 1033.

We also appreciate the *Interagency Statement on the Use of Alternative Data in Credit Underwriting*,[1] which was issued in December 2019 by the CFPB along with the Federal Reserve Board, FDIC, Office of the Comptroller of the Currency, and National Credit Union Administration. The Interagency Statement encourages the use of cash flow data as one of the more promising forms of alternative data, while cautioning that some types of data could present "greater consumer protection risks." The Statement takes a nuanced, careful approach, which is important for the treatment of bank account transaction information.

A nuanced, careful approach is critical because the intensely detailed and sensitive data inside consumers' accounts can also be used for less beneficial purposes. It could help predatory lenders refine their ability to make and collect on unaffordable loans or allow consumers to be targeted for products that do not improve their well-being. It could be sold or shared to debt collectors to figure out the best time to collect debts by analyzing when income comes in and can be grabbed. Transaction data can also be fed into algorithms or machine learning with results that lead to discrimination.

NCLC has written extensively on these risks and the guardrails that are necessary to ensure that consumers benefit, and are not harmed by, the use of bank account transaction data. The following summarizes these concerns, which are set forth more fully in the attached documents:[2]

1. Need for oversight

As discussed below, there are a number of areas where data aggregators need more oversight, including data security, privacy, and compliance with consumer reporting and fair lending laws. Yet to our knowledge, no one – not even likely states – is examining data aggregators. That should change. While the industry is still in its relative infancy, the CFPB has the opportunity to ensure that it benefits consumers and does not harm.

The CFPB should engage in a rulemaking to establish supervisory authority over the larger participants in the data aggregator market. The CFPB has authority over data aggregators as

[1] https://files.consumerfinance.gov/f/documents/cfpb_interagency-statement_alternative-data.pdf.
[2] These attachments are: (1) Testimony of Lauren Saunders, National Consumer Law Center, Before the U.S. House of Representatives Committee on Financial Services - Task Force on Financial Technology regarding "Banking on Your Data: The Role of Big Data in Financial Services" November 21, 2019, https://www.nclc.org/images/pdf/cons-protection/testimony-lauren-saunders-data-aggregator-nov2019.pdf ; and (2) Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048, Feb. 2017, https://www.nclc.org/images/pdf/rulemaking/comments-response-data-aggregator.pdf.

providers of account information,[3] as material service providers,[4] or as providers of a product or service that will likely have a material impact on consumers.[5] If the data aggregator is a consumer reporting agency, as discussed below, they may already be a larger participant in the consumer reporting market and should be examined.

2. Data security

Data security is obviously critical in any system that accesses or uses consumers' account data. Still today, access is often gained by using the consumers' username and password to access the account (also known as "screen scraping"). More recently, many data aggregators have worked to strike agreements with financial institutions to access account data through secure automated programming interfaces (APIs), but many institutions are still not covered. We support efforts to increase the use of APIs and eliminate screen scraping, and we are participating in an initiative to set standards for APIs: the Financial Data Exchange (FDX). The CFPB should support and encourage efforts to move away from screen scraping.

Data security by both the data aggregator and the ultimate end user are also critical. As part of CFPB supervision, there should be an examination of data security on the part of data aggregators, using the same authority that the Bureau is currently exercising to examine the nationwide consumer reporting agencies for data security.

3. Unauthorized charges

It is critical that consumers' right to contest unauthorized charges – directly through their financial institution, not the data aggregator – be respected. In the past, some financial institutions have taken the position that consumers lose their dispute rights and liability protection if they give a third party permission to access their account and unauthorized charges result. That is incorrect and the CFPB should make that crystal clear.

4. Portability

Consumers may wish to access their account data not only for add-on services used in connection with their accounts but also for purposes of closing the account and transferring it elsewhere. Setting up bill payments for a variety of other accounts, redirecting preauthorized charges, and even collecting and storing transaction information can be a cumbersome process. The control that financial institutions have over account data, and the difficulty of moving it elsewhere, inhibits competition and locks consumers into accounts with which they are unhappy. The CFPB should facilitate mechanisms to enable consumers to access their data to enable comparison shopping and switching providers.

[3] 12 U.S.C. § 5481(15)(A)((ix).
[4] 12 U.S.C. § 5481(26).
[5] 12 U.S.C. § 5481(15)(A)(x).

5. Consumer Choice, Control and Protection

Consumers face the risk of losing control and privacy when they provide access to their account data. Consumers may believe that they are providing access only for purposes of a narrow range of or time-limited transactions or services. But the third party can gain access to 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. Creditors could use this information to make decisions based on where the consumer shops (i.e., dollar stores vs high end boutiques) instead of the individual's credit risk. Access may go on far longer than expected by a consumer who envisioned a one-time or limited access.

While data aggregators currently seek consumers' consent, consent alone does not provide consumers with sufficient protection. Today, people can easily choose to avoid products that require use of a data aggregator. But as the use of access to account information spreads, refusing to click "I agree" will become much harder, just as consumers do not truly have any power to say no if a potential employer wants to pull a credit report.

First and foremost, there must be substantive limits on how companies can use data that cannot be superseded by blanket consent:

- **Companies should not be allowed to use purported consent to permit uses that consumers do not expect or understand**.
- **Use must be limited by purpose**. A consent to use bank account data for credit underwriting should extend to that use alone and should not permit the use of the data for other purposes such as marketing, debt collection, or government licensing.

Consent should also be a product of real choice:

- **Consumers should always have true choice in whether to share their bank account data.** There is too great a risk that creditors will require use of bank account transaction data for all consumers, including those who could have received credit without it. A consumer who already has a "fat file" and a good credit score should be able to rely on that alone without being required to share bank account information. Expansion into bank account information may benefit those consumers who have insufficient credit history information or lower credit scores, but could hurt or risk the privacy of consumers who already qualify for mainstream credit.
- **Consumers should never be required to share bank account transaction data for non-credit purposes**, such as employment, insurance, or government licensing or benefits. Needs-based government programs should be entitled to only a snapshot of current balances.
- **Consent must be real, knowing and meaningful.** It should never be buried in fine print. It must always be in a separate stand-alone document.

Consumers also need more control over how and when they provide consent or revoke consent:

- **Consent must be limited by data element.** A consumer should be able to choose sharing just cash flow information (credits, debits, balances) versus sharing cash flow plus the identities of merchants from debit card transactions or the identity of payors who make electronic deposits.
- **Consent should be time-limited and self-expiring.** A consent for credit underwriting should be a single use permission. A consent for account review for an open-end account should expire after one year and require renewal.
- **Consumers should have multiple, simple options for ending data sharing.** Some banks and data aggregators are developing consumer dashboards where they can see who is accessing their data and easily turn it off. Multiple access points – at the bank, at the data aggregator, and at the end user app – are necessary. Most consumers do not know who a data aggregator is, and their bank will be the most logical place for them to look. But only the data aggregator may know the multiple other accounts – investment, credit, savings – that may be accessed by an app.

6. Fair Lending Considerations

It is critical that the data accessed by data aggregators, like other data, not be used in a fashion that results in discrimination or disparate impacts on consumers in vulnerable communities. Account data will almost certain exhibit disparities by race because one of the factors used by scoring models is likely to be overdrafts, and African Americans are disproportionately affected by bank overdraft practices.[6]

As discussed above, bank accounts can include a host of sensitive information, including what neighborhoods and stores the consumer shops in. Location or geographic neighborhood is one way that creditors have inappropriately assessed creditworthiness by association.[7] The type of store or establishment a consumer frequents may also reflect race or ethnicity.

Thus, use of account data could lead to racial or other disparities not based on the individual's credit risk. This is especially true when data that correlates with race or other protected classes

[6] See Pew Charitable Trusts, Heavy Overdrafters, April 2016, at 7http://www.pewtrusts.org/~/media/assets/2016/04/heavyoverdrafters.pdf?la=en (African-Americans are 12 percent of the US population, but account for 19 percent of the heavy overdrafters).

[7] Jeffrey S. Morrison & Andy Feltovich, Leveraging Aggregated Credit Data and in Portfolio Forecasting and Collection Scoring, The RMA Journal, Oct. 2010, at 47, available at www.forecastingsolutions.com/publications/RMA_OCT2010.pdf (article written by Transunion researchers stating "…aggregated credit data is…helpful to [debt] collectors because it can identify local credit conditions clustered around common demographics. This is especially true for consumers with little or no credit history. For example, if the consumer is living in a ZIP code where the mortgage delinquency rates are climbing or always high, the chance for collection may be significantly less than for those in ZIP codes where the delinquency rate is relatively low and stable.").

is fed into opaque algorithms and machine learning. There is an assumption that algorithms are automatically unbiased or judgment free, but recent research indicates otherwise.[8] Recent studies and news reports have shown that computers can discriminate too, from digital mortgages[9] to Apple credit cards.[10]

Data that is used for credit purposes – including data obtained through data aggregators – is subject to the Equal Credit Opportunity Act (ECOA). Data that is using in housing decisions – as bank account cash flow data theoretically could be – is subject to the Fair Housing Act (FHA). Data that results in disparate impacts in other areas may be subject to other federal or state anti-discrimination laws. The CFPB should ensure that the use of consumers' account data does not result in discriminatory impacts against consumers in any context

Actively looking out for and preventing inappropriate disparate impacts is essential. Only by looking for broad patterns can we ensure that we are not perpetuating discrimination and inequality through digital redlining.

II. Regulatory Issue: Applicability of the Fair Credit Reporting Act

One of the contentious issues regarding the role of data aggregators has been coverage under the Fair Credit Reporting Act (FCRA). As those familiar with the FCRA know, the terms "consumer report" and "consumer reporting agency" under the Act are not limited to the "Big Three": Equifax, Experian, and TransUnion. Instead, the terms are broad and expansive, covering entities such as criminal background check vendors, tenant screening agencies, and deposit account screening databases. These terms also apply to new technology companies such as data aggregators that provide third party information used for credit underwriting or other FCRA covered purposes.

If a company is collecting and sharing third-party data that is used or expected to be used as a factor in determining eligibility for credit, insurance, employment, or other purposes authorized

---

[8] *See* Carol Evans, Federal Reserve Board - Division of Consumer and Community Affairs, Keeping Fintech Fair: Thinking about Fair Lending and UDAP Risks, Consumer Compliance Outlook - Second Issue 2017 (2017), https://consumercomplianceoutlook.org/2017/second-issue/keeping-fintech-fair-thinking-about-fair-lending-and-udap-risks/ ("while statistical models have the potential to increase consistency in decision-making and to ensure that results are empirically sound, depending on the data analyzed and underlying assumptions, models also may reflect and perpetuate existing social inequalities. Thus, big data should not be viewed as monolithically good or bad, and the fact that an algorithm is data driven does not ensure that it is fair or objective.").

[9] *See* Robert P. Bartlett, et al., Consumer Lending Discrimination in the FinTech Era, UC Berkeley Public Law Research Paper, December 7, 2017, https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf (finding that fintech lenders discriminate, albeit 40% less than face-to-face lenders).

[10] *See* Will Knight, Wired, The Apple Card Didn't 'See' Gender—and That's the Problem: The way its algorithm determines credit lines makes the risk of bias more acute (Nov. 19, 2019), https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem.

under the FCRA, that company should be considered a "consumer reporting agency" or CRA subject to the FCRA. The term CRA extends to:

> any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.
>
> 15 U.S.C. § 1681a(f).

A key term in this definition is that the consumer reporting agency's activities must be for the purpose of furnishing "consumer reports." Information is a consumer report if it is:

- Pertains to any of seven characteristics, which cover an extremely far-reaching range of information – credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, and mode of living;
- Used or expected to be used or collected in whole or in part to serve as a factor in establishing eligibility for consumer credit or other FCRA-covered purposes
- Issued by consumer reporting agency.

15 U.S.C. § 1681a(f).

Thus, almost all third-party data collected for credit decision-making purposes should be considered a "consumer report," and the entity that furnishes the data to third parties is a "consumer reporting agency."

FCRA protections are critical to protecting consumers when data is used to evaluate them for credit. One of the key issues with alternative data is the level of accuracy of the data. Although one might assume that information drawn from consumers' bank accounts will be accurate, that might not always be the case as errors might arise as the data is passed along, especially with screen scraping. Indeed, the seventh principle in the CFPB's *2017 Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* is Accuracy, which is stated as "Consumers can expect the data they access or authorize others to access or use to be accurate and current. Consumers have reasonable means to dispute and resolve data inaccuracies, regardless of how or where inaccuracies arise."

The FCRA addresses the very issues in this seventh principle. The FCRA requires CRAs to follow "reasonable procedures to ensure maximum possible accuracy." 15 U.S.C. § 1681e(b). The Act also gives consumers the right to dispute any errors regarding information about them in a CRA's files. 15 U.S.C. § 1681i(a).

Some have argued that the FCRA does not apply to data aggregators because consumers must generally provide affirmative consent or permission for their account data to be accessed by the aggregators. However, consent or the lack thereof is not an element of the definition of

"consumer report" or "consumer reporting agency." Indeed, it would create a huge loophole in the scope of FCRA coverage to exempt data collected with the consumer's consent from coverage as a consumer report. Every loan agreement would include a consent to share information in the fine print so that the information would not be considered a consumer report when gathered by the Equifax, Experian and TransUnion. Not only would this exempt the Big Three from the scope of "consumer reporting agency," it would exclude the lender from consideration as a furnisher – thus providing lenders with a huge incentive to include such buried, fine print consents in their agreements.

Another argument has been that aggregators are not CRAs because they act as a "dumb pipe" that is merely a conduit for information and thus does not meet the element of "assembl[ing] or evaluat[ing]" information in the definition of a consumer reporting agency. However, the Federal Trade Commission has defined "assembling" to mean "gathering, collecting, or bringing together consumer information such as data obtained from CRAs or other third parties, or items provided by the consumer in an application."[11] This description specifically fits the activities of data aggregators, since they "collect" or "gather" information from third parties. Indeed, the very word "aggregator" means to "someone or something that gathers together materials from a variety of sources."[12]

Finally, there has been an argument that data aggregators are not CRAs because arguably the banks from which account data is provided are not furnishers under the FCRA[13] given that the information is taken or "pulled" from them. However, the fact that information is gathered from a passive source of information, as opposed to being transmitted by a furnisher, does not exclude a company from coverage under the FCRA. For example, some criminal background check companies pull or scrape data from court records or other public sources. Yet these entities are clearly considered consumer reporting agencies even though the court or government agency did not "furnish" or transmit the information to the background check CRA.[14]

The potential lack of a furnisher does introduce a wrinkle for an aggregator to fulfill its dispute handling duties under the FCRA. The Act requires a CRA, when it receives a consumer's dispute

[11] Federal Trade Commission, 40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations 29, July 2011, https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf. [hereinafter "FTC 40 Years Report"]

[12] Definition of 'aggregator', Merriam-Webster, https://www.merriam-webster.com/dictionary/aggregator (visited February 11, 2020).

[13] For more on the argument that a bank from which account transaction data originates is not a "furnisher" under the FCRA, *see* Kwamina Thomas Williford & Brian J. Goodrich, Why Data Sources Aren't Furnishers under Credit Report Regs, hklaw.com (Sept. 25, 2019).

[14] The FTC has stated that "[a]n entity whose record searchers collect publicly available information such as criminal records for employer screening of applicants, then forwards the information to its headquarters where a report is prepared consisting of that information, has conducted "assembling" activities sufficient to meet the definition of a CRA." FTC 40 Years Report at 29.

over the accuracy or completeness of information, to send a notice of the dispute to the furnisher and involve the furnisher in the dispute investigation. 15 U.S.C. § 1681i(a)(2). Without a furnisher, there is no entity for a CRA to involve in a dispute. However, CRAs that pull information from public records sources face similar issues, and yet are able to conduct dispute investigations. Furthermore, this could be an issue that a rulemaking under Section 1033 could address.

* * * * * *

Thank you for the opportunity to submit this statement and to participate in the Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act. If you have questions about this statement, please contact me at cwu@nclc.org or 617-542-8010.

Respectfully submitted,

Chi Chi Wu
National Consumer Law Center
(on behalf of its low income clients)