Testimony before the

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES
Task Force on Financial Technology

Regarding

"Preserving the Right of Consumers to Access Personal Financial Data"

September 21, 2021

Chi Chi Wu

Staff Attorney

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

7 Winthrop Square, 4th Fl.

Boston, MA 02110

617-542-8010

cwu@nclc.org

Testimony of Chi Chi Wu,
National Consumer Law Center
Before the U.S. House of Representatives Committee on Financial Services
Task Force on Financial Technology
regarding
"Preserving the Right of Consumers to Access Personal Financial Data"
September 21, 2021

Chairman Lynch, Ranking Member Davidson, and Members of the Financial Technology Task Force, thank you for inviting me to testify today regarding preserving the right of consumers to access personal financial data. I offer my testimony here on behalf of the low-income clients of the National Consumer Law Center.[1]

Introduction

There has been a tremendous amount of interest in the growing use of data from consumers' bank accounts and other financial accounts to provide a variety of financial products and services, generally facilitated by third parties called "data aggregators." This topic is the subject of a rulemaking from the Consumer Financial Protection Bureau (CFPB) under Section 1033 of the Dodd-Frank Act,[2] which requires banks and other financial services providers to make financial account data available to the consumer, subject to CFPB rules. The Section 1033 rulemaking has garnered a significant amount of attention and even a mention in President Biden's Executive Order on competition.[3]

We support the call in President Biden's Executive Order for CFPB to continue the Section 1033 rulemaking. Access to consumers' financial account data has the potential to enable many products and services that may be beneficial to consumers. At the same time, the intensely detailed and sensitive data inside consumers' financial accounts can also be used for less beneficial purposes, such as debt collection or targeting consumers for predatory or exploitative products. Data also must be shared in a secure fashion, safe from unauthorized access and data breaches. Whether access to financial account data benefits or harms consumers will depend on whether the CFPB's 1033 rule, rules by other federal agencies, and any new legislation contain

---

[1] The National Consumer Law Center is a nonprofit organization specializing in consumer issues on behalf of low-income people. We work with thousands of legal services, government and private attorneys, as well as community groups and organizations, from all states who represent low-income and elderly individuals on consumer issues. *Fair Credit Reporting* (9th ed. 2017) is one of the eighteen practice treatises that NCLC publishes and annually supplements. This testimony was written by Chi Chi Wu, with the assistance and editorial review by Lauren Saunders.

[2] *See* CFPB, Consumer Access to Financial Records, 85 Fed. Reg. 71003, 71011 (Nov. 6, 2020).

[3] Executive Order on Promoting Competition in the American Economy, July 9, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/ ("The Director of the Consumer Financial Protection Bureau, consistent with the pro-competition objectives stated in section 1021 of the Dodd-Frank Act, is encouraged to consider: (i) commencing or continuing a rulemaking under section 1033 of the Dodd-Frank Act to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products").

strong consumer protections that ensure the three "C"s and one "D" for access to this valuable source of information:

- **C**onsumer Choice and Control
- **C**ompetition
- **C**onsumer Protection
- **D**ata Security

Background: Benefits and Risks of Financial Account Data

Many stakeholders have promoted the benefits of consumer-authorized financial account information for various purposes, including the 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. Our primary focus has been on the use of financial account data for purposes of credit underwriting.

Use of financial account data could benefit the 45 million "credit invisible" consumers who lack a credit history or have files so skimpy that a credit score cannot be generated.[4] Financial account data could allow credit invisible consumers to obtain affordable credit based on an analysis of the cash flows in the consumers' bank or prepaid card accounts, *i.e.*, the pattern of debits and credits and balances. Cash flow data has shown significant promise as a form alternative data for underwriting, perhaps the most promising form.[5] Indeed, the CFPB, along with the other banking regulators, has encouraged the use of cash flow data because of this underwriting potential, cautioning that other types of data could present "greater consumer protection risks."[6]

There are indications that credit invisible customers of larger banks already have an on-ramp to credit because of cash flow data. It appears that larger banks may be approving credit cards based on deposit account information at their own institutions.[7] Customers of smaller banks or banks that do not issue credit cards do not have the same benefit. Consumer-authorized data access could level that playing field.

---

[4] Kenneth Brevoort, Philipp Grimm & Michelle Kambara, CFPB Office of Research, CFPB Data Point: Credit Invisibles 12 (May 2015), http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf.

[5] FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings (July 2019), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

[6] CFPB, Federal Reserve Board, FDIC, Office of the Comptroller of the Currency, and National Credit Union Administration, *Interagency Statement on the Use of Alternative Data in Credit Underwriting* (December 2019), https://files.consumerfinance.gov/f/documents/cfpb_interagency-statement_alternative-data.pdf.

[7] Data Point: Becoming Credit Visible, June 2017, https://files.consumerfinance.gov/f/documents/BecomingCreditVisible_Data_Point_Final.pdf, at 33 (noting that "about 65 percent [of consumers studied], appear to have transitioned out of credit invisibility by opening an account by themselves despite their lack of a credit history" and that "perhaps some commercial banks are willing to lend to credit invisible consumers with whom they have existing deposit account relationships.").

In addition to credit underwriting, access to account data could allow consumers to more easily change financial institutions. 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. Consumers should have access to their data to enable comparison shopping and switching providers.

However, access to the financial account data also poses risks to consumers. The intensely detailed and sensitive data inside consumers' accounts can also be used for less beneficial purposes. Some predatory lenders may use the timing and history of inflows and outflows from consumers' accounts to fine tune their ability to collect, but not necessarily the consumers' ability to afford credit while meeting other expenses. Financial account data could even 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.

A consumer's deposit account contains a wealth of information about the consumer's 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.[8]

Financial account data has been touted as a means to promote financial inclusion, and research has found that it holds promise for helping borrowers of color who might otherwise face constraints on their ability to access credit.[9] However, there still will be disparities by race given the unequal economic positions of households of color and white households, as well as racial disparities in the impact of overdraft practices, as discussed on page 9. When financial account data is fed into algorithms or artificial intelligence models, the results could replicate those disparities.

Whether financial account data ultimately benefits consumers will depend on how vigorous the rights and protections for consumers are. Consumers must have choice and control over our own data; competition must flourish and not be stifled; consumer protections must be strong and forceful; and data security requirements must be robust.

[8] For example, a professor at U.C. Berkeley's Haas Business School found that "spending on entertainment (such as video, audio, magazines, newspapers, toys and pets) predicts worse credit outcomes. Spending on categories that predict worse consumer credit outcomes tend to also predict smoking and lower education (proxies for impatience), suggesting that impatience is central for consumer credit outcomes." This research could prompt creditors to examine a consumer's purchases in underwriting, leading to lower approvals or higher prices for pet owners or consumers with too many streaming subscriptions. Annette Vissing-Jorgensen, Consumer Credit: Learning Your Customer's Default Risk from What (S)he Buys, Aug. 20, 2021, http://faculty.haas.berkeley.edu/vissing/VissingJorgensenConsumerCredit2021.pdf

[9] FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings (July 2019), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

Element 1: Consumer Choice and Control

The most important principle for access to financial account data is that it must always be the consumer's choice, and consumers should have full control over their information. *Pro forma* consent is not sufficient; the decision must be an affirmative, knowing, and conscious decision. Consumers should also have the power to shut off the data spigot and to delete the information if they change their mind, as well as the power decide what data elements will be shared.

While data aggregators currently seek consumers' consent, this alone is not sufficient. First, it is unclear whether consent as currently obtained from consumers is truly knowing and voluntary. When consumers click "I agree," many do not understand they are turning over all their deposit account data to a third party. A November 2019 survey by The Clearing House (TCH) found that 80% of financial app users were not aware that apps may use third parties to access consumers' financial information.[10]

Even when consumers do truly consent knowingly and voluntarily, they may assume the data will only be used for the immediate purpose for which they authorized accessed. They may not realize the access is not limited to that purpose; that more data may be accessed than is necessary; or that access may not be restricted in time but could continue indefinitely. Access may go on far longer than expected by a consumer who envisioned a one-time or limited access.

Consent may not be truly voluntarily if the consumer is forced to provide it as a condition of obtaining the credit or services, even when account data is not necessary such as when a consumer has a thick credit file with a high credit score. Today, people can easily choose to avoid products that require use of a data aggregator. But as the use of access to financial 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.

Finally, consent is not actually required by any statutory scheme, even the Gramm-Leach-Bliley Act (GLBA), which only provides for an opt-out of sharing. It is competitive forces that compel banks not to share this data, and such forces could shift with a change in the market. Indeed, there is currently a project that would use data from the consumer reporting agency Early Warning Services (EWS) to supply cash flow information for credit invisible consumers via the Big Three credit bureaus (Equifax, Experian, TransUnion). While this project does have benefits for these consumers, consent will not be required for creditors to obtain the EWS data. This lack of consumer control is less preferable to a system where the consumer must give permission to access to their financial account information, as it deprives consumers of the autonomy over their data.

To avoid the risks to consumer control, privacy, and misuse of their data, the following principles must be followed.

---

[10] Statement of Natalie S. Talpas, PNC Bank, for CFPB Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, February 26, 2020, https://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdf (citing The Clearing House, Consumer Survey: Financial Apps and Data Privacy, November 2019).

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

1. Data aggregators and data users should not be allowed to use purported consent to permit uses that consumers do not expect or understand.
2. Use by data aggregators and data users must be limited by purpose. A consent to use deposit account data for credit underwriting 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:

3. Consumers should always have true choice in whether to share their deposit account data as a substitute or supplement for a credit score. Creditors and other users should not be permitted to require consumers to share bank transaction data if they could have received credit or other services without it.
4. Aggregators should not be permitted to share deposit account transaction data for non-financial purposes, such as employment, insurance, or government licensing or benefits. Needs-based government programs should be entitled to only a snapshot of current balances.
5. Consent must be real, knowing, affirmative, and meaningful. It should never be buried in fine print. It must always be in a separate stand-alone "document," *i.e.*, webpage or dashboard. The role of the aggregator must be disclosed in a manner that consumers realize it is a separate third-party intermediary that is accessing their account data.

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

6. Consent must be limited by data element (i.e., data minimization). A consumer should be able to control sharing of 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. Not every use case needs all of the information in a consumer's account, and users should only receive what they need for their application to function properly.
7. 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.
8. Consumers should have multiple, simple options for ending data sharing and deleting information. Some banks and data aggregators are developing consumer dashboards where consumers 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.

Element 2: Competition

Consumer-permissioned bank account data could represent a paradigm shift in assessing the creditworthiness of consumers. For decades, consumers and their data have been held captive to abuses and exploitation by the Big Three credit bureaus, *i.e.*, the nationwide consumer reporting

agencies (CRAs). The credit bureaus have created a credit reporting system that has unacceptably high levels of errors as well as a biased and dysfunctional dispute system.[11]

There is a frequent refrain that the consumer is not the customer of the credit bureaus; instead, our data is their commodity. Our consent is never required to harvest our information and, until the advent of security freezes, we could not even prevent its dissemination. The credit reporting system is an oligopoly of three companies where market forces do not work and consumers have no choice but to be beholden to those companies.

That all has the potential of changing with consumer-authorized data from deposit and financial accounts. This is a source of data that can serve as potential competition to the credit bureaus. It may be more predictive. It could be more accurate than credit bureau data, not only because the source is drawn directly from the consumer's deposit account but because consumers could have more control over it. Consumers must authorize access to the data, and as discussed above, they should have the ability to shut off access whenever they want. If an aggregator does a terrible job with the accuracy of data, the consumer should have the ability to revoke authorization and delete their data from the aggregator's database.

Consumer control would not only help with accuracy as a curative measure, it would help with incentives to ensure accuracy on a prospective basis. If an aggregator knows that too many errors will result in consumers revoking their authorization and deleting their data, the aggregator is likely to take measures to ensure and improve accuracy.

American consumers desperately need to have an alternative to the Big Three credit bureaus. That competition could come from aggregators of consumer-authorized data. Of course, one risk that we are already beginning to see is that the Big Three have started purchasing alternative data providers. For example, Experian purchased Clarity while TransUnion purchased FactorTrust and Equifax purchased Teletrack. All three of the purchased companies are CRAs focused on subprime credit. In other cases, the credit bureaus form partnerships with alternative data providers to access their data. Equifax has a partnership with Yodlee, while Experian has a deal with Finicity, both of which are data aggregators.

While *partnerships* may be understandable, it would be another matter and very troubling if the Big Three creditors actually purchased these and other data aggregators. Anti-trust enforcement of such sales and acquisitions is critical.

Moreover, if bank account data flows through the credit bureaus, even if the initial use is cash flow underwriting, the result could be simply more data in consumer credit reports over which consumers lose control. Simply adding more data to the credit reporting system is less beneficial than having new alternative sources to create competition. And if data gets incorporated into credit reports or is sold and resold, consumers may not even be aware of new uses, let alone have the protection of needing to consent.

[11] *See* NCLC, Automated Injustice Redux: Ten Years after a Key Report, Consumers Are Still Frustrated Trying to Fix Credit Reporting Errors, Feb. 25, 2019, https://bit.ly/ajustre.

Element 3: Consumer Protection

It is clear that existing consumer protection laws apply in the context of consumer authorized account data. If used for credit underwriting, the Fair Credit Reporting Act (FCRA) applies and the Equal Credit Opportunity (ECOA) is implicated. The Electronic Funds Transfer Act (EFTA) applies if unpermissioned access to data leads to an unauthorized charge, or if a financial institution using shared data makes a payment or deposit error.

Some stakeholders have claimed that there is regulatory uncertainty as to the applicability of these laws, which they argue impedes innovation.[12] We do not believe that the application of existing laws is either uncertain or a negative circumstance hindering innovation. We have seen many examples over the years of new entrants asserting that well-established statutes do not apply to them because they use novel innovations or technology. They ignore the fact that despite being drafted several decades ago, the federal consumer protections are written broadly, and their core elements generally do not hinge on specific technologies. They are not limited to depository institutions or brick & mortar lenders.

1. Electronic Funds Transfer Act

The most critical principle with respect to EFTA is this one: the use of data aggregators should not deprive consumers of their protection against unauthorized charges or other errors, nor make it more difficult for the consumer to invoke their EFTA rights to correct errors and reverse unauthorized charges. Of the stakeholders in authorized data access, the consumer is least able to bear the cost of a loss. As we all well know, many consumers live paycheck to paycheck, with 40% of Americans who would struggle with an unexpected $400 bill.[13] Many consumers cannot afford the unexpected loss that would occur if their EFTA rights were undermined in the fights between financial institutions and data aggregators.

The CFPB recently clarified several questions that have arisen regarding unauthorized transfers that occur as a result of data sharing. The CFPB stated that a transfer is unauthorized within the meaning of Regulation E, and the consumer is protected from liability, even if the consumer was fraudulent induced into sharing account access information or if the consumer was negligent. The CFPB also stated that a financial institution cannot rely on a modification or waiver of

[12] The CFPB reflected back these concerns in its Advanced Notice of Proposed Rulemaking for Section 1033. *See* CFPB, Consumer Access to Financial Records, 85 Fed. Reg. 71003, 71011 (Nov. 6, 2020). The CFPB also recently clarified several questions arising under the EFTA regarding unauthorized transfers that arise out of data sharing. *See* CFPB, Electronic Fund Transfers FAQs, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/.

[13] Federal Reserve Board, Report on the Economic Well-Being of U.S. Households in 2018 - May 2019; Dealing with Unexpected Expenses, https://www.federalreserve.gov/publications/2019-economic-well-being-of-us-households-in-2018-dealing-with-unexpected-expenses.htm.

Regulation E liability protections in the account agreement on the basis that the consumer has shared account information with a third party.[14]

Consumers also are not in a position to prevent unauthorized charges or other errors that could occur through use of a data aggregator. Nor should they be caught in the middle of a finger pointing exercise between the financial institution, the data aggregator, and the data user. The consumers' right to contest unauthorized charges and to dispute error directly through their financial institution must be respected.

2. Equal Credit Opportunity Act

Data accessed by aggregators, like any other alternative data, must not be used in a fashion that results in discrimination or disparate impacts on consumers in vulnerable communities. Deposit account data will almost certainly exhibit disparities by race. For one thing, a key factor likely to be used by scoring models is overdrafts, and Black consumers are disproportionately affected by bank overdraft practices.[15] **Indeed, the ability of cash flow data to help minority and low-and moderate-income consumers will not bear fruit unless and until bank overdraft abuses are brought to an end.**

As discussed above, deposit 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.[16] 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 is fed into opaque algorithms and machine learning. There is an assumption that algorithms are automatically unbiased or judgment free, but research indicates otherwise.[17] Studies and news

[14] *See* CFPB, Electronic Fund Transfers FAQs, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/.

[15] *See* Pew Charitable Trusts, Heavy Overdrafters, April 2016, at 7, http://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).

[16] 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.").

[17] *See* Elisa Jillson, Federal Trade Commission Aiming for Truth, Fairness, and Equity in Your Company's Use of AI, Apr. 19, 2021, https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai ("Advances in artificial intelligence (AI) technology promise to revolutionize our approach to medicine, finance, business operations, media, and more. But research has highlighted how apparently "neutral" technology can produce troubling

reports have shown that computers can discriminate too, from mortgage automated underwriting systems[18] to healthcare delivery.[19]

Data that is used for credit purposes – including data obtained through data aggregators – is subject to the ECOA. Data that is using in housing decisions – as 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 or laws against unfair, deceptive, or abusive practices.

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.

3. 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 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 (ChexSystems, EWS). These terms also can apply to new technology companies, including data aggregators that provide third party information used for credit underwriting or other FCRA covered purposes. Indeed, a major data aggregator has also taken the position that aggregators are likely covered as CRAs when their data is used for credit underwriting.[20]

Despite being 50 years old and the first federal privacy law, the FCRA has withstood the test of time. It was written broadly, based on basic principles of fair information practices:

---

outcomes – including discrimination by race or other legally protected classes"; discussing various studies documenting AI producing racial disparities).

[18] *See* Emmanuel Martinez and Lauren Kirchner, The Secret Bias Hidden in Mortgage-Approval Algorithms, The Markup, Aug. 25, 2021, https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms ("Holding 17 different factors steady in a complex statistical analysis of more than two million conventional mortgage applications for home purchases, we found that lenders were 40 percent more likely to turn down Latino applicants for loans, 50 percent more likely to deny Asian/Pacific Islander applicants, and 70 percent more likely to deny Native American applicants than similar White applicants. Lenders were 80 percent more likely to reject Black applicants than similar White applicants").

[19] *See* Eliane Röösli, Brian Rice, Tina Hernandez-Boussard, Bias at Warp Speed: How AI May Contribute to the Disparities Gap in the Rime of COVID-19, Journal of the American Medical Informatics Association, Vol. 28, Issue 1, January 2021, https://doi.org/10.1093/jamia/ocaa210 ("In this frenzy, the risk of producing biased prediction models due to unrepresentative datasets and other limitations during model development is higher than ever. If not properly addressed, propagating these biases under the mantle of AI has the potential to exaggerate the health disparities faced by minority populations already bearing the highest disease burden.").

[20] Finicity, FCRA and Data Agents White Paper, Feb. 11, 2001, https://www.finicity.com/fcra-data-agents/.

- *The right to have information be accurate:* The FCRA requires "reasonable procedures for maximum possible accuracy" from consumer reporting agencies.
- *The right to correct errors:* Consumers have the right to dispute inaccurate information and get it corrected.
- *The right to access information about ourselves*: The FCRA gives consumers the right to disclosure of information about themselves in the files of a consumer reporting agency.
- *The right to know when information is used against us*: Consumers get an "adverse action" notice when information in the form of a consumer report is used to deny them credit, employment, insurance, rental housing, or many other financial essentials.
- *Privacy protections to prevent inappropriate dissemination and use*: Only users with a "permissible purpose" can access consumer reports.

The accuracy and error resolution provisions are among the most critical FCRA protections applicable to data aggregation. Although one might assume that information drawn from consumers' deposit accounts will be accurate, that might not always be the case as errors might arise as the data is processed and passed along, especially with screen scraping. The FCRA requires CRAs to follow reasonable procedures to ensure maximum possible accuracy, 15 U.S.C. § 1681e(b), and when information is not accurate, gives consumers the right to dispute any errors and seek resolution, 15 U.S.C. § 1681i(a). These FCRA rights must be preserved when financial account data is used for credit or other FCRA-covered purposes.

The FCRA also has specific notice requirements, which are intended to ensure transparency when information from a CRA is used. Mostly importantly, Section 615(a) and (h) of the Act, 15 U.S.C. § 1681m(a) and (h), require users of consumer reports to provide adverse action and risk-based pricing notices when information from a CRA has been used to deny them credit or charge them a higher price. This ensures that consumers are aware of the sources and types of information that are used against them in credit (and other) decisions, so that they are not left in the dark as to the reasons for decisions that may have critical consequences for their lives.

Finally, if financial account data is a consumer report when it is used for credit underwriting, that same data from the same data aggregator CRA is still a consumer report if used for other purposes.[21] To the extent that data from an aggregator is never used for an FCRA-covered purpose and is never part of a consumer report, similar fair information rights are necessary, *i.e.,* accuracy, dispute rights, file disclosures, and notices. However, it is critical that any regulation setting up a separate system of rights not undermine FCRA coverage. If there is uncertainty as to whether certain data qualifies as a "consumer report," any regulation should explicitly provide that nothing in it shall be construed to limit or restrict the applicability of the FCRA. FCRA coverage is preferable because it is a time-proven statute with an established body of law and clear, enforceable consumer rights.

[21] *See* National Consumer Law Center, Fair Credit Reporting § 2.2.5.4 (9th ed. 2017), updated at www.nclc.org/library.

4. Data aggregators should be subject to CFPB Supervision

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. While the industry is still in its relative infancy, the CFPB has the opportunity to ensure that it benefits consumers and does not cause harm.

Thus, we have advocated that as part of the Section 1033 rulemaking, the CFPB should issue a rule establishing supervisory authority over the larger participants in the data aggregator market. The CFPB has authority over data aggregators as providers of account information,[22] as material service providers,[23] or as providers of a product or service that will likely have a material impact on consumers.[24] If the data aggregator is a CRA, it may already be a larger participant in the consumer reporting market and should be examined.

Element 4: Data Security

Data security is obviously critical in any system that accesses or uses financial account data. There should be data security obligations on the part of both the aggregator and the end user.

1. Screen Scraping vs APIs

With consumer-authorized data, access is often gained by using the consumers' username and password to access the account (often referred to as "screen scraping"). Screen scraping is less than optimal from a data security perspective; this is one reason we believe the industry should move away from screen scraping.

Many data aggregators have worked to strike agreements with financial institutions to access account data through secure automated programming interfaces (APIs). There appears to be universal support that data aggregation should move away from screening scraping and toward APIs. Consumer groups support efforts to increase the use of APIs and eliminate screen scraping, and consumer groups have been participating in the Financial Data Exchange (FDX).

However, screen scraping should not be prohibited unless and until all consumers at every financial institution have the right and ability to access their own data using more secure means such as an API. A prohibition on screen scraping without such universal access would give banks and other institutions the upper hand and ability to prematurely shut out access.

2. Data Security

Data security is obviously critical in any system that accesses or uses consumers' account data. The main governing law for data security is the Gramm-Leach-Bliley Act (GLBA).

[22] 12 U.S.C. § 5481(15)(A)((ix).
[23] 12 U.S.C. § 5481(26).
[24] 12 U.S.C. § 5481(15)(A)(x).

In terms of regulatory regimes, CRAs are subject to the Federal Trade Commission's Safeguards Rule, and data aggregators are likely subject to that rule as well. The FTC Safeguards Rule is currently the subject of a rulemaking to strengthen its requirements.[25] Congress should urge the FTC to complete this rulemaking to improve data security for CRAs, data aggregators, and other non-bank entities.

However, even with enhanced protections, the Safeguard Rule and FTC's authority over data security are missing a critical element – supervision, which the FTC has neither the authority nor the infrastructure to conduct. As discussed above, the CFPB could supervise data aggregators, and already supervises larger participant CRAs - but GLBA specifically excludes the CFPB from jurisdiction over its data security provisions.[26] Since the Equifax data breach in 2017,[27] we have urged Congress to transfer the GBLA data security authority to the CFPB for CRAs, and we would urge the same with respect to data aggregators.

* * * * *

Financial account information holds great promise but also great risk. It could open the doors to credit for millions of underserved Americans, including consumers of color, as well as help facilitate competition. It could also result in products and innovations that benefit consumers and enable portability of financial accounts.

There is a dark side to the sharing of account data, though. It could also lead to unwanted wider and wider access to consumers' private data. The nightmare scenario is a system where every consumer - thin or thick file, high FICO score or not - must automatically give up the privacy of their bank account information and allow each creditor, employer, landlord, insurer, and government agency a direct and permanent digital pipeline to their bank account data. It is up to the regulators, and ultimately Congress, to make sure that this data promotes consumer welfare without harming our best interests.

Thank you again for the opportunity to provide my views to the Task Force today. I look forward to your questions.

Supplemental materials

(1) NCLC, etc. Comments to the CFPB in Response to the ANPR Regarding Consumer Access to Financial Records Under Section 1033 of the Dodd-Frank Act, Feb. 4, 2021, https://www.nclc.org/images/pdf/credit_reports/Comments_CFPB_1033_ANPR.pdf.

[25] 84 Fed. Reg. 13158 (Apr. 4, 2019).
[26] *See* 15 U.S.C. §§ 6801(b), 6805(b)(1). The CFPB could and may already be supervising the CRAs for data security under other authority, such as the prohibition against unfair, abusive or deceptive practices under Section 1031 of the Consumer Financial Protection Act.
[27] Testimony of Chi Chi Wu before the U.S. House of Representatives, Committee on Financial Services, regarding Examining the Equifax Data Breach (Oct. 25, 2017), https://www.nclc.org/images/pdf/credit_reports/nclc-tstmny-hfsc-equifax-hearing-102517.pdf.

(2) NCLC Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, February 12, 2020, https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf

(3) 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

(4) NCLC 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