Testimony 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

Lauren Saunders
Associate Director

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

1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
202-595-7845
lsaunders@nclc.org

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

Summary

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

Today I would like to focus on the 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. 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.

At the same time, the intensely detailed and sensitive data inside consumers' accounts can also be used for less beneficial purposes. It may help predatory lenders refine their ability to make and collect on unaffordable loans or allow consumers to be targeted for products that do not

[1] Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people, including older adults, in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitive practices, help financially stressed families build and retain wealth, and advance economic fairness.

improve their well-being. Transaction data can also be fed into algorithms or machine learning with results that lead to discriminatory impacts.

The use of data aggregators poses a number of questions and concerns regarding:

- Safe methods of accessing and storing data;
- Privacy, whether information is used in ways consumers would expect, and whether consumer choice and control are meaningful;
- Consumers' rights under the Fair Credit Reporting Act to know what information is being used, to demand accuracy, to obtain corrections, and to know when information results in adverse consequences; and
- Disparate impacts that result in discrimination against disadvantaged communities.

A number of efforts are underway to address many of these issues, including the work of Financial Data Exchange (FDX). While voluntary efforts by industry are welcome, ultimately consumers cannot have confidence that their data will be used in appropriate ways unless the law clearly protects them across these different dimensions. In particular, we support:

- Enhanced data security requirements for all entities, federal supervision of entities that store significant amounts of consumer data, and respect for consumer's right to contest unauthorized charges;
- A strong federal privacy law that does not preempt state privacy protections;
- Application of the FCRA to new forms of data access and collection;
- Disparate impact analysis for use of big data, enforcement of the Equal Credit Opportunity Act (ECOA), and protection against disparate impacts when data is used for purposes other than credit; and
- A greater role for the Consumer Financial Protection Bureau in supervising data aggregators for compliance with all applicable laws within its jurisdiction and enforcing privacy and data security standards.

A. Data Aggregators and the Use of Consumers' Account Data

In the past few years, data aggregators such as Plaid, Yodlee and Finicity have increasingly enabled companies, with consumer permission,[2] to access consumers' bank account, credit account, investment account and other account data in order to enable a growing variety of products and services.[3] These data aggregators are not typically consumer-facing, but rather operate behind the scenes to provide other companies with information from consumer's financial accounts. Many of products and services offered by these financial technology ("fintech") and other companies show promise to benefit consumers. But uses of this data should be monitored, as there are many possible worrisome uses of and impacts of this data.

1. Credit scoring and cash-flow underwriting

Data aggregators, both directly and through partnerships with the big three credit reporting agencies, offer access to transaction data for purposes of underwriting credit. Transaction data may supply information that is not normally considered, such as utility or rent payments, or may be used to analyze the consumers' cash flow.

Some services, like ExperianBoost, may draw on bank account transaction data to enable lenders to consider a consumer's utility payments, which typically do not get included in traditional credit reports.[4] Consumer-permissioned access to bank account transaction data is a better way to incorporate utility payment data than full-file utility reporting, which risks harming the scores of millions. Consumers who want creditors to consider their utility payments can grant access without pushing utility companies to report all payments for all consumers, which raises a host of

[2] *But see* section C below on the limits of consumer "permission."
[3] For a discussion of some of the "fintech" companies that use data aggregators, see Lauren Saunders, National Consumer Law Center, Fintech and Consumer Protection: A Snapshot (March 2019), http://bit.ly/2Tx9BmG.
[4] Susan Henson, Experian, Introducing Experian Boost, a New Way to Instantly Improve Your Credit Scores, April 8, 2019, https://www.experian.com/blogs/ask-experian/introducing-experian-boost/. Other services access certain utility, telecom and cable data from other sources, sometimes with consumer permission. *See, e.g.*, Press Release, Equifax Continues Leadership In Alternative Data With Worldwide Urjanet Partnership Financial Information (Sept. 18, 2019), https://investor.equifax.com/news-and-events/news/2019/09-18-2019-122941123 ; FICO, FICO Score XD, https://www.fico.com/en/products/fico-score-xd.

issues including harmful impact on credit scores for many and interference with state utility shutoff protections.[5]

Other services incorporate the full range of bank account transaction data into credit scores or cash-flow underwriting. UltraFICO relies on bank account transaction information from Finicity, a data aggregator working in partnership with Experian.[6] For now at least, UltraFICO will only be used to enhance a consumer's credit scores to see whether a denied application can be approved or a lower rate can be offered. A partnership between Equifax and Yodlee uses real-time bank account information like balances, deposits and withdrawals to augment other credit data. Some lenders, such as Petal, may also use data aggregators directly to access bank account transaction data.

Access to bank account transaction data can enable cash-flow underwriting, a potentially positive form of underwriting. Analysis of a consumer's actual inflows and outflows, income and expenses can be used alone or together with traditional credit reports to assess whether a consumer has the ability to repay credit.[7] A look at the consumer's actual residual income may provide a realistic picture of whether the consumer regularly has sufficient funds at the end of the month to handle a loan payment or, conversely, whether the consumer has difficulty meeting expenses.

Cash-flow data may help those who do not have significant credit histories. Indeed, a CFPB study has speculated that that one of the primary "on ramps" to a credit report might be the consumer obtaining their first credit card from their own bank.[8] The use of a data aggregator for

[5] *See, e.g.*, Letter from 40 associations, consumer, civil rights and advocacy groups to U. S. House of Representatives (Dec. 8, 2017), opposing H.R. 435, which would preempt state laws that do not permit utilities to submit payment information to credit bureaus, https://www.nclc.org/images/pdf/legislation/letter-oppose-hr435-hfsc.pdf; Comments of consumer groups in Response to Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process, Docket No. CFPB-2017-0005, at 3 to 5 (May 19, 2017), https://www.nclc.org/images/pdf/credit_reports/comments-alt-data-may2017.pdf

[6] FICO, Introducing UltraFICO, https://www.fico.com/ultrafico/ (viewed July 21, 2019).

[7] *See* FinRegLab, The Use of Cash-Flow Data in Underwriting Credit (July 2019), at 3 https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf (noting that cash-flow scores "frequently improved the ability to predict credit risk among borrowers that are scored by traditional systems as presenting similar risk of default").

[8] Consumer Financial Protection Bureau, Data Point: Becoming Credit Visible, June 2017, https://files.consumerfinance.gov/f/documents/BecomingCreditVisible_Data_Point_Final.pdf, at 33 (noting that

account information allows this access even when a consumer does not have a deposit account at a large bank that also issues credit cards.

Analysis of transaction data may provide a way to underwrite consumers whose income comes from informal or irregular sources that is otherwise difficult to document. Transaction data can also substitute for more cumbersome methods of documenting income.

Cash-flow data may help consumers who are recovering from a temporary setback. Bank account data can avoid the need to rely on credit scores that reflect negative marks from economic hardships years ago.[9] Data suggests that many of the consumers with impaired credit were the victims of unfortunate events such as illness or job loss.[10] Bank account data can show when there has been a healthy sustained recovery from an economic shock such as a job loss or illness.

Today, most of these uses of cash-flow data only kick in to enhance a consumer's credit score in order to see if a consumer who was denied can be approved or if the consumer can be given a lower rate. They have the ability to help consumers without exposing them to the risk of lower credit scores or harming their existing credit report. Consumers also generally permission use of their data for a particular credit application.

However, with some services there are questions as to whether the consumer's opt in will allow ongoing use by any lender that accesses the service – or by the credit bureau more broadly – potentially in ways that the consumer does not expect or understand. It is also not clear that, as time goes on, all of these uses of cash-flow underwriting will only enhance a consumer's credit

---

"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.")

[9] Lenders often review 12 months of statements at most even when they manually review bank account activity For example, Fannie Mae requires lenders to review 12 months of bank account statements to establish payment activity. Fannie Mae Selling Guide, B3-5.4-03: Documentation and Assessment of a Nontraditional Credit History, August 30, 2016, *available at* https://www.fanniemae.com/content/guide/selling/b3/5.4/03.html. Anecdotally, we have heard that some lenders only require 3 to 6 months of bank account statements.

[10] About 70 to 80% of consumers with impaired credit or a low score, such as a 600, will actually not default. These may be victims of extraordinary life circumstances who do not default again once they have recovered economically. *See* Chi Chi Wu, NCLC, Solving the Credit Conundrum: Helping Consumers' Credit Records Impaired by the Foreclosure Crisis and Great Recession, Dec. 2013, at 9-11, *available at* www.nclc.org/images/pdf/credit_reports/report-credit-conundrum-2013.pdf (summarizing research).

score rather than decrease it. These broader uses of transaction data for credit underwriting bear monitoring, especially in light of the dismal record of the credit reporting agencies in being overly aggressive in selling the sensitive financial information of consumers.[11] The temptation to maximize the monetary value of this data will be significant.

2. Other uses of account transaction data.

Personal financial management services may use account transaction data to help consumers save or invest. Services can manage the inflows and outflows of consumers' accounts, identify when there are extra funds potentially available, and make it easy to transfer those funds to a savings or investment account.

Data aggregators can enable account verification when a consumer wishes to link an account for a person-to-person payment service, savings device, or other purpose. This linkage can be accomplished faster and easier than through older methods, such as using micro deposits that the consumer must wait for and then verify. Account data can also be used for identity verification in other contexts.

Other services allow consumers to better manage their money and identify or avoid bank fees. Some apps help consumers anticipate and cover upcoming bills or prevent or address overdrafts.[12] Other services consolidate bank, credit, investment, and other account information so that consumers can see the entire picture of their finances in one place.

Data aggregators can help companies provide competition for banks. Consumers can be a captive audience for banks, which have an edge over competitors due to the information they

[11] For example, the FTC spent many years battling TransUnion over its sale of target marketing lists. *See* Trans Union Corp. v. F.T.C., 245 F.3d 809 (D.C. Cir. 2001) (upholding FTC's ruling and discussing history of the case). Consumer advocates have argued for many years that the practice of prescreening is nothing more than using consumer reports for marketing. *See* National Consumer Law Center, Fair Credit Reporting § 7.3.3 (9th ed. 2017), *updated at* www.nclc.org/library.

[12] I will not in this testimony address concerns about products that are offering credit in the guise of other services not covered by credit laws. *See* Fintech and Consumer Protection, *supra*.

hold on consumers. Data aggregators enable fintechs to reach consumers and compete, and also push banks to improve their own services.

Eventually, data aggregators may make it easier for consumers to close their bank account and transfer it elsewhere.[13] 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 inhibit competition and lock consumers into accounts with which they are unhappy. Data aggregators might be able to help consumers easily transfer the data they need to a new account.

At the same time, not all of the potential uses of consumers' account transaction data are positive.

Enabling lenders to push more credit on consumers with subprime credit scores may not always be a good thing. It could instead lead people to become more overburdened by debt and in a worse position to manage their finances. Underwriting models that focus on the risk to the creditor are not the same thing as affordability by the consumer. Some lenders may access the timing and history of inflows and outflows from consumers' accounts to fine tune a predatory lenders' ability to collect but not necessarily the consumers' ability to afford credit. And for some purposes, credit invisibility could be better than a negative profile, such as a history of overdrafts, which could harm consumers in seeking employment and or in insurance pricing.[14] Thus, we would advocate that account transaction data not be used for these purposes.

Some of the services offered through data aggregators may be mere pretenses to harvest consumer data that can be used for product pitches or other purposes. Companies may claim to

[13] *See* Suzanne Martindale et al., Consumers Union, Trapped at the Bank: Removing Obstacles to Consumer Choice in Banking (May 30, 2012), https://advocacy.consumerreports.org/wp-content/uploads/2013/09/TrappedAtTheBank1.pdf.
[14] *See* Testimony of Chi Chi Wu before the U.S. House of Representatives, Committee on Financial Services, Task Force on Financial Technology, regarding Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit (July 2019), https://www.nclc.org/images/pdf/credit_reports/testimony-alternative-data-credit-scoring.pdf.

be making offers in the consumers' best interest when they instead are motivated by advertising revenue or revenue sharing. Debt settlement products and others that frequently end up harming consumers finances could be pushed on consumers.

Consumers could eventually be required to provide access to their account data for use by employers, insurers, and other purposes not imagined today. Government agencies could even require "Big Brother" monitoring of purchases and spending as a condition for government benefits.

And, as discussed in section E below, account transaction data can also be used in ways that result in disparate impacts on vulnerable communities.

B. Data security and protection from unauthorized charges are critical.

Data security is obviously critical in any system that accesses or uses consumers' account data. Security issues are posed by the method of accessing that data; how the data is stored and shared; and how consumers are protected if there is a problem.

In the early days of account aggregation, access was typically 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). While APIs are a superior form of account access, bilateral agreements between individual data aggregators and individual financial institutions take time to negotiate.[15] Screen scraping continues to be used if the consumer has an account at one of the vast number of financial institutions that do not yet have an API set up with the particular data aggregator. We support efforts to increase the use of

[15] We are aware of concerns by data aggregators that financial institutions in these bilateral agreements may impose limits on the types or frequency of data that may be accessed. We take no position in these debates, but we do note, as discussed in section C below, that aggregators and the fintechs they work with should only access the minimum data needed, for the minimum amount of time, needed to perform the function that the consumer expects and authorizes.

APIs and eliminate screen scraping. Regulators may be able to play a role in facilitating these efforts.

Data security by both the data aggregator and the ultimate end user are also critical. The data aggregator may obtain the consumers' username and password even if an API is ultimately used, and the data accessed through account aggregation also is very sensitive and must be held securely. While data aggregators promise high levels of security, and many impose security requirements on end users, consumers have no capacity to evaluate the trustworthiness, security protocols, motives or activities of either data aggregators or the companies that offer services based on account data.

Even the largest banks with the most robust compliance regimes – that are subject to the data security rules of Graham Leach Bliley Act and are examined by the bank regulators -- have been subject to data breaches. Voluntary promises of data security by data aggregators are simply insufficient.

While consumers have legal protection against unauthorized charges, that does not mean that they will not be harmed by a data breach. Disputes about unauthorized charges can take time to resolve, depriving consumers of access to their funds in the meantime. Banks do not always believe consumers when they contest unauthorized charges. Data breaches can also harm consumers in other ways, such as by opening them up to potential identity theft for years into the future.

Congress must extend data security and privacy rules beyond the current scope of financial institutions under Gramm-Leach Bliley. It is also well past time to give federal regulators the authority and the mandate to begin regular data security examinations of consumer reporting agencies, data aggregators, and other companies that hold significant amounts of sensitive consumer data.

It is also 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.[16] Consumers still retain protection against unauthorized charges just as they would if they gave their debit card to their child who then is mugged. If the breach ultimately happened at the data aggregator or fintech end user, then the bank and data aggregator or other company can work out who should bear the ultimate liability. But with new data breaches happening every day, consumers have no way of knowing how an unauthorized charge happened. They must retain the right to go to the institution that holds the account to resolve the issue.

C. Privacy, consumer choice and control must be meaningful.

Beyond security risks, consumers also face privacy risks when they provide access to their account data. Consumers may believe that they are providing access only for purposes of a narrow range of 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. Some services harvest this information for marketing purposes and even at times may reserve the right to share it with or sell it to other parties that the consumer does not contemplate.

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 an employer wants to pull a credit report. Plus, if data gets incorporated into credit reports or is sold and resold, consumers may not even have the minimal control of providing consent for new uses.

[16] *See* Comments of National Consumer Law Center (on behalf of its low income comments) in Response to Request for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (Feb. 21, 2017), https://www.nclc.org/images/pdf/rulemaking/comments-response-data-aggregator.pdf.

Consent alone is also insufficient because the vague privacy policies that consumers receive do not give them any real idea of how their information may be used. Consumers should not be expected to decipher privacy policies to hunt for inappropriate uses. Consumers also may have used a service once or twice to try it out and long forgotten about it, not realizing their information is still being collected and potentially disseminated. While consumers have the right to limit data sharing with unrelated third parties, they are often unaware of those rights, and may have difficulty knowing how to change their preferences.

Congress and federal regulators must act to enhance consumers' privacy. Privacy issues plague a wide variety of financial and nonfinancial services, though they are particularly acute given the sensitive information that may be obtained through access to a financial account.

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. Both access points – at the bank and the data aggregator – 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.

We appreciate that there are industry efforts to achieve more consumer control over data sharing. Again, while voluntary efforts are helpful in the short run, that will not achieve uniform protections or consumer confidence. Ultimately only clear rules of the road with which all actors must comply will fully protect consumers.

Finally, any federal privacy bill must not preempt stronger protections at the state level. Privacy issues evolve, and no bill will ensure protection into the future. States are more nimble in addressing new problems and can provide the laboratory of democracy for trying new solutions.

D. Consumers need FCRA protections for use of their data

The Fair Credit Reporting Act (FCRA) gives consumers important rights to know what information is being used about them, to ensure that that data is accurate, to require those collecting information to correct errors, and to learn when use of information results in adverse consequences. These rights are important not only for traditional credit reports but also for newer information sources such as the account information accessed through data aggregators.[17]

The FCRA was intended to have a very broad scope of coverage. Information is a "consumer report" covered by the FCRA if it is:

- 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 (including "a legitimate business need");
- 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; and
- Issued by a third party that regularly assembles or evaluates such data for money or on a nonprofit cooperative basis.

Thus, almost all third-party data collected for credit decision making purposes should be considered a "consumer report." Unfortunately, several circuit courts have shown a reluctance to respect the plain language of the FCRA and its broad coverage.[18] **We urge Congress to re-**

[17] The FCRA also limits the dissemination of consumer report information to entities with a "permissible purpose," fairly broadly defined. 15 U.S.C. § 1681b(a). However, as discussed in Section C above, there should be greater protections and consumer control for financial account data.

[18] *See* Kidd v. Thomson Reuters, 925 F.3d 99 (2d Cir 2019)(CLEAR product was not a consumer report, despite state agency's use for employment purposes, because Thomson Reuters had collected information and intended it to be used only for non-FCRA purposes, expressly prohibited its sale or use for FCRA-related purposes, required users to make non-FCRA use certifications, and actively monitored compliance; entity must have a specific intent to furnish a "consumer report,"); Zabriskie v. Fed. Nat'l Mortg. Ass'n, 940 F.3d 1022 (9th Cir. 2019) (in a 2-1 decision, holding that Fannie Mae's Desktop Underwriter program is not a CRA because Fannie Mae did not act with the purpose of furnishing consumer reports to third parties but instead to facilitate a transaction between the lender and itself; relying on *Kidd v. Thomson Reuters* to require specific intent to furnish a consumer report)); Fuges v. Southwest Title, 707 F.3d 241 (3d Cir. 2012) (objectively reasonable for company that prepared reports on current owners of properties to interpret the reports as outside the FCRA because they allegedly pertained to the property and not to the consumer -- despite the fact the reports included information on judgments personally against the consumer).

affirm the broad scope of the FCRA and that it applies to any-third party data used for credit evaluation purposes.

FCRA protections are critical to protecting consumers when data is used to evaluate them for credit. One of the key issues with alternative data 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, or inaccurate conclusions might be drawn from that data. The FCRA requires accuracy, in that Section 607(b) of the FCRA, 15 U.S.C. § 1681e(b), requires consumer reporting agencies (CRAs) to follow "reasonable procedures to ensure maximum possible accuracy." Section 611(a) of the FCRA, 15 U.S.C. § 1681i(a), gives consumers the right to dispute any errors regarding information about them in a CRA's files.

The FCRA also has specific notice requirements, which are intended to ensure transparency when information about consumers is used. Mostly importantly, Section 615(a) and (h) of the Act, 15 U.S.C. § 1681m(a) and (h), require users to provide adverse action and risk-based pricing notices when information has been used to deny credit or charge 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.

Furthermore, even if third party information is somehow not considered a consumer report, the FCRA includes a little-known provision that requires transparency in its usage. Section 615(b), 15 U.S.C. § 1681m(b), requires that lenders provide a specific notice if information that fits any of the seven characteristics listed in the definition of "consumer report" is obtained from a person other than a consumer reporting agency and is used to deny credit or charge more for it. This notice must inform the consumer of the right to make a written request for the reasons for the adverse action. Upon such a request, the user must disclose the nature of such information. Section 615(b) should apply to alternative data used for credit decision making even if it somehow escapes the definition of a consumer report.

While banks that use information in a consumer's account at that bank are not covered by the FCRA, data that is not the product of direct experience between the lender and the consumer should be regulated by the FCRA. Compliance with the FCRA is critical for the purposes of accuracy, predictiveness, transparency, and appropriate use.

E. Account data is covered by the ECOA and can result in disparate impacts.

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. African Americans are disproportionately affected by bank overdraft practices.[19] And beyond balances and the mere inflow and outflow of funds, bank and credit accounts have a host of sensitive information.

Bank and credit accounts can identify what neighborhood the consumer shops in. Location or geographic neighborhood is one way that creditors have inappropriately assessed creditworthiness by association.[20] Given the degree of residential housing segregation that exists in the U.S., location can function as a proxy for race and income and its use by creditors would reflect racial and socio-economic disparities.

Account data can also identify what types of stores, websites or services a consumer uses, or what causes she supports – all of which may correlate with race or other protected classes.[21] It is

[19] *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).

[20] 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.").

[21] The use of behavioral data has shown indications of racial bias, despite relying on seemingly racially neutral algorithms. In 2013, Latanya Sweeney, a professor of government at Harvard University, led a research project that concluded that Google searches of names more likely associated with black people often yielded advertisements for a criminal records search in that person's name. Hiawatha Bray, Racial bias alleged in Google's ad results, Boston

even conceivable that account data could reveal who a consumer's friends are and who she exchanges funds with.[22]

Thus, use of accounts data could lead to racial or other disparities not based on the individual's credit risk.[23] 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 recent research indicates otherwise.[24] Recent studies and news reports have shown that computers can discriminate too, from digital mortgages[25] to Apple credit cards.[26]

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.[27]

Globe (February 6, 2013) https://www.bostonglobe.com/business/2013/02/06/harvard-professor-spots-web-search-bias/PtOgSh1ivTZMfyEGj00X4I/story.html.

[22] While the information accessed through data aggregators will not directly include social media information, it is possible that data aggregators could identify social circles through the information in payment accounts like Venmo. *Cf*. Katie Lobosco, Facebook friends could change your credit score, CNN.com (August 27, 2013) *available at* http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html. *See also* Matt Vasilogambros, "Will Your Facebook Friends Make You a Credit Risk?" The Atlantic (August 7, 2015), https://www.theatlantic.com/politics/archive/2015/08/will-your-facebook-friends-make-you-a-credit-risk/432504/.

[23] *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/ ("[F]intech may raise the same types of fair lending risks present in traditional banking, including underwriting discrimination, pricing discrimination, redlining, and steering. Although some fintech trends may decrease certain fair lending risks, other trends could amplify old problems or create new risks.") [hereinafter "Evans, *Keeping FinTech Fair*"]

[24] *See* Evans, *Keeping FinTech Fair* ("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.").

[25] *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).

[26] *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/.

[27] *See* Comments of civil rights, consumer, and other advocacy organizations on Request for Information Regarding the CFPB's Inherited Regulations and Inherited Rulemaking Authorities, Docket No. CFPB-2018-0012 regarding Regulation B and the Equal Credit Opportunity Act (June 25, 2018), https://www.nclc.org/images/pdf/rulemaking/cfpb-inherited-regs-disparate-impact.pdf.

As one fintech, Lending Club, put it, disparate impact is an innovation friendly approach:

> [T]he disparate impact regime …
> (a) can address a widely held policy concern [that credit decisioning technology may discriminate without people intending or realizing it] while flexibly accommodating innovation in data, machine learning, and artificial intelligence (AI),
> (b) has not been onerous to comply with in our experience, and
> (c) provides the regulatory stability that supports innovation and investment.[28]

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. **Congress should ensure that the use of consumers' data does not result in discriminatory impacts against consumers in any context.**

Like the FCRA, the ECOA is a statute with a broad scope. It prohibits discrimination "with respect to any aspect of a credit transaction" on the basis of, *inter alia*, race, color, religion, national origin, sex or marital status, or age. 15 U.S.C. § 1691(a). "Credit" is broadly defined, as is the concept of "creditor," which is not limited to banks or traditional lenders. 15 U.S.C. § 1691a(d) and (e). Finally, the ECOA is not limited to consumer credit but applies to certain types of business credit as well.

Most importantly for our purposes, Regulation B, which implements the ECOA, expressly notes that "legislative history of the Act indicates that the Congress intended an 'effects test' concept … be applicable to a creditor's determination of creditworthiness." 12 C.F.R. § 1002.6(a). The

[28] *See* Comments of Lending Club to Consumer Financial Protection Bureau re: Request for Information Regarding the Bureau's Inherited Regulations and Inherited Rulemaking Authorities; Maintain Disparate Impact Policy (June 23, 2018), https://www.regulations.gov/document?D=CFPB-2018-0012-0075; Comments of the National Consumer Law Center, et al. to the U.S. Department of Housing and Urban Development on HUD's Implementation of the Fair Housing Act's Disparate Impact Standard, Docket No. FR-6111-P (August 19, 2019), https://www.nclc.org/images/pdf/special_projects/racial_justice/comments-to-hud-disparate-impact-standard-oct2019.pdf.

effects test is another name for the disparate impact test, and the Official Staff Interpretations explain that the test:

> may prohibit a creditor practice that is discriminatory in effect because it has a disproportionately negative impact on a prohibited basis, even though the creditor has no intent to discriminate and the practice appears neutral on its face, unless the creditor practice meets a legitimate business need that cannot reasonably be achieved as well by means that are less disparate in their impact.

Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.6(a)-2. This effects test essentially has a three-step analysis that consists of:

1. Does the practice have a disproportionately negative impact on a protected class even if it appears neutral on its face?
2. If so, does the practice meet a legitimate business need?
3. Can the same need be reasonably achieved using a less discriminatory alternative?

Like the FCRA, the ECOA also has specific notice requirements. It requires creditors to notify consumers of the action on an application. 15 U.S.C. § 1691(d)(1). If the creditor takes an adverse action, it must provide either a statement of reasons for the action or written notification of the right to such a statement. 15 U.S.C. § 1691(d)(2). This notice must be specific, and must meet the requirements of Regulation B and its corresponding Official Staff Interpretations.[29]

The notices required by the FCRA and ECOA raise one of the key issues with regards to the use of account data and other forms of alternative data, especially if they are used in artificial intelligence or machine learning – transparency.

[29] Reg. B, 12 C.F.R. § 1002.9(b)(2); Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(2). *See generally* National Consumer Law Center, Credit Discrimination § 10.5.4.2 (6th ed. 2013), *updated at* www.nclc.org/library.

Consumers are entitled to know not only *what* information is being used to assess them, but *how* that information is being used. The use of data aggregators must not reinforce and entrench existing inequality.[30]

F. The CFPB Should Supervise Data Aggregators

Data aggregators are playing a growing role in consumers' lives. While the industry is still in its relative infancy, data aggregators can impact consumers in many of the same ways that credit reporting agencies can.

As discussed above, there are a number of areas where data aggregators need more oversight, including data security, privacy, and compliance with credit reporting and fair lending laws. Yet to our knowledge, no one – not even likely states – is examining data aggregators.

That should change. The Consumer Financial Protection Bureau has authority over data aggregators as a provider of account information,[31] as a material service provider,[32] and as a provider of a product or service that will likely have a material impact on consumers.[33] The CFPB should define the larger participants[34] in the data aggregator market and should supervise them for compliance with all applicable laws within the CFPB's jurisdiction. In addition, as discussed above, the CFPB should already be examining data aggregators that are within the FCRA's definition of "consumer reporting agency" to the extent they are larger participants in the credit reporting market.

We also support proposed legislation to expand the data aggregators that are subject to the Graham Leach Bliley Act's safeguard rules[35] and to give the CFPB authority to establish standards under the Act and to enforce data aggregators' compliance. The FTC does not have a

[30] A list of studies is available in Chi Chi Wu, NCLC Past Imperfect: How Credit Scores and Other Analytics "Bake In" and Perpetuate Past Discrimination (May 2016), https://www.nclc.org/images/pdf/credit_discrimination/Past_Imperfect050616.pdf.
[31] 12 U.S.C. § 5481(15)(A)((ix).
[32] 12 U.S.C. § 5481(26).
[33] 12 U.S.C. § 5481(15)(A)(x).
[34] 12 U.S.C. § 5514(a)(1)(B), (a)(2).
[35] 15 U.S.C. § 6801(b).

supervision regime, and there is no reason that data aggregators should not be subject to GLBA supervision the way banks and credit unions are.

* * * * *

The myriad new uses of consumers' account data through data aggregators are intriguing and many will benefit consumers. But we must not allow ourselves to be led down the primrose path of opening up wider and wider access to our personal data without keeping our eyes wide open to where it might lead.

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

Lauren Saunders
Associate Director
National Consumer Law Center
On behalf its low income clients