National Consumer Law Center
(on behalf of its low-income clients)
Americans for Financial Reform Education Fund
Center for Responsible Lending
Consumer Action
Consumer Federation of America
USPIRG

February 4, 2021

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

Re: Consumer Access to Financial Records, Docket No. CFPB–2020–0034/RIN 3170-AA78.

The National Consumer Law Center (on behalf of its low-income clients) (NCLC), Americans for Financial Reform Education Fund, Center for Responsible Lending, Consumer Action, Consumer Federation of America, and USPIRG are pleased to submit these comments in response to the Consumer Financial Protection Bureau (CFPB)'s Advanced Notice of Proposed Rulemaking regarding Consumer Access to Financial Records, Docket No. 2020-0034, issued November 6, 2020. The CFPB has requested comment on 46 questions to assist it in developing a proposed rule to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act. These comments address a selected number of these questions that we as consumer advocacy groups are particularly suited to answer. In summary, these comments discuss how:

1. The potential benefits for consumers of authorized data access, assuming strong provisions for consumer control, security, and use limitations, are significant, as consumer use of their own data could provide a better alternative and provide true competition to the Big Three credit bureaus. The CFPB should issue a strong rule under 1033 to ensure protections for consumers accessing their own account data.

2. Authorized data access also poses significant risks to consumers. Consumers face the dangers of losing control over the data, having it used against them, and having their privacy invaded. The type of consent currently obtained by data aggregators and the lack of limits on use of that data leave consumers vulnerable to abuse, exploitation, and security risks. The CFPB must issue strong rules mandating true consumer control over their own data, substantive

limits on how companies can use and share data, and meaningful choice over whether consumers want to share that data.

3. The CFPB should encourage aggregators to move away from screen scraping and should encourage financial institutions to accept data sharing through application programming interfaces (APIs), but the Bureau cannot prohibit screen scraping until all consumers at any financial institution have the ability to access their own data through APIs. The CFPB should set broad-based standards for authorized data access, such as a common data dictionary, or require the establishment of industry-wide standards. The CFPB should ensure data security through supervision of data aggregators and data users; also, aggregators should be governed by the FTC Safeguards Rule issued under Gramm-Leach-Bliley Act.

4. The CFPB should guarantee that consumers are protected when their account data is accessed and used by companies. It should exercise supervisory authority over data aggregators, and ensure application of strong protections under the Electronic Funds Transfer Act, Equal Credit Opportunity Act, and the Fair Credit Reporting Act.

5. The CFPB should adopt rules under Section 1033 to give consumers the right to information beyond deposit account data, such as: (a) a copy of the consumer report or risk score that a covered person used in connection with providing the consumer a financial product or service; (b) records retained by a covered person pursuant to Regulation Z or Regulation B; and (c) behavioral data sold by the credit bureaus to covered persons for marketing purposes.

Finally, NCLC has written extensively on the risks involved with the use of the financial account transaction data for which they authorize access, and the guardrails that are necessary to ensure that consumers benefit and are not harmed by such use. These concerns are set forth more fully in the following documents, which are both attached and incorporated by reference:

(1) 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

(2) 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

(3) 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

A. The Benefits and Risks of Authorized Data Access to Consumers and Competition (Questions 1, 2 and 3)

The potential benefits for consumers of authorized data access are significant, but the potential risks are also great. In order to realize the benefits to consumers while minimizing the risks for consumers, the CFPB must issue a strong rule under Section 1033 that include vigorous, substantive safeguards for consumers.

Our response to Questions 1 through 3 about benefits and risks to consumers and competition primarily focus on the use of consumer-authorized financial account data for purposes of credit underwriting. Other comments, particularly by Consumer Reports, focus on the benefits and risks to consumers generally with respect to a range of uses for authorized data, including facilitating payments and personal financial management. For these use cases, the benefits may not be as great and the risks may be different; thus, the benefit-risk calculation may also be very different.[1] In those cases, it is even more important that the CFPB issue strong rules to prevent the risks discussed by both our comments.

1. Ensuring that evolution and innovation benefit consumers

We are on the cusp of another 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.[2] In 2017, lax data security at Equifax permitted hackers to steal the sensitive financial information of 148 million consumers.[3]

There is a frequent refrain that the consumer is not the customer of the credit bureaus; instead, our data is their commodity. Consumers have no control in this system. 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.

---

[1] Some of these concerns are also discussed in 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" at 8-9 (Nov. 21, 2019), https://www.nclc.org/images/pdf/cons-protection/testimony-lauren-saunders-data-aggregator-nov2019.pdf.

[2] 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.

[3] Government Accountability Office, Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach, GAO-18-559, (Aug. 2018), https://www.gao.gov/assets/700/694158.pdf.

That all has the potential of changing with consumer-authorized data from deposit accounts. This is a source of data that can serve as potential competition to the credit bureaus. It may be more predictive, the proverbial better mousetrap. Access to consumer-authorized data allows an analysis of the cash flows in the consumer's deposit account, *i.e*., the pattern of debits and credits and balances. Cash flow data has shown significant promise as a form alternative data, perhaps the most promising form.[4] Indeed, the CFPB, along with the other banking regulators, has encouraged the use of cash flow data because of this potential, cautioning that other types of data could present "greater consumer protection risks."[5]

In addition, account data 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 in Section B.2 below, the CFPB should equip them with the meaningful ability to shut off access whenever they want. If an aggregator does a terrible job with the accuracy of data, a Section 1033 rule should ensure that consumers 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.

2. Cost and Risks to Consumers

Of course, use of authorized account data for credit underwriting 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. High-cost lenders that use cashflow underwriting irresponsibly could lead thin or no file consumers to have a visible but negative credit score – putting them on the map for predatory actors, or damaging their ability to obtain jobs or insurance.

As more and more creditors require consumers to authorize access to account data in order to obtain credit, any consumer consent could become no more meaningful than being forced to click "I agree" to pages of fine print. Moreover, when account data flows through the credit bureaus, even if the initial use is cashflow underwriting, the result could be simply more data in consumer credit reports over which consumers lose control.

---

[4] 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.

[5] 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.

Authorized account 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. Account data can also be fed into algorithms or machine learning with results that lead to discrimination, discussed in Section D.2 below.

To avoid these dangers to consumer control and privacy, the CFPB must include the limitations discussed in Section B and D below in any Section 1033 rulemaking. Authorized data access also presents risks to consumers from data breaches or unauthorized transactions due to lax security. Data security risks are discussed in Section C.3 below.

3. Strong rules over access to authorized data are necessary to ensure that competition benefits consumers

Improved access to consumer-authorized data can benefit competition, which will benefit consumers. A strong Section 1033 rule is necessary to achieve this benefit.

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, both of which are CRAs focused on subprime credit. In some cases, the credit bureaus form partnerships with alternative data providers to access their data. Equifax manages NCTUE, while Experian has a deal with Finicity, a data aggregator. While such partnerships are understandable, it would be another matter and very troubling if the Big Three actually purchased these and other data aggregators. While the CFPB does not have authority over anti-trust enforcement, it does have authority to promote fair competition and its views, should be influential on this issue.

Without consumer-authorized data access, lenders may turn to sources of deposit account data that are both less consumer friendly and ultimately harm smaller financial institutions. For example, there appears to be an effort to promote the use of the account screening CRA Early Warning Services (EWS) to supply cashflow information via the Big Three nationwide CRAs. This is suboptimal for several reasons – (1) there may be significant FCRA compliance issues regarding reseller, file disclosure, and adverse action notice requirements; (2) lack of an authorization requirement means a lack of consumer control; and (3) using EWS limits the benefits of cashflow analysis to customers of the big banks that are part of the EWS cooperative, giving those banks an undue competitive advantage.

Thus, addressing Question 11, safe authorized data access with strong consumer controls could benefit "credit invisible" customers of smaller banks because they will be able to take advantage of underwriting based on their deposit accounts via aggregators. First, this access will prevent the benefit of cashflow analysis from being limited to the larger banks that comprise EWS. Second, there are indications that credit invisible customers of larger banks

already have an "on ramp" to a credit file because the larger banks will approve a credit card based on deposit account information at their own institution.[6] Customers of smaller banks or banks that do not issue credit cards do not have the same benefit. Consumer-authorized data access will level that playing field.

4. Section 1033 Rules Should Ensure Account Portability as a Benefit

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. This is all the more important as financial institutions push consumers to relinquish paper statements in favor of electronic information that may disappear after the account is closed. 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 Section 1033 rule should facilitate mechanisms to enable consumers to access their data to enable comparison shopping and switching providers.

B. Consumer Choice and Privacy (Questions 25 through 32; Question 17)

1. Threats to consumer control and privacy

Consumers face significant risks of losing control and privacy when they provide access to their account data. While data aggregators currently seek consumers' consent, consent alone does not provide consumers with sufficient protection for several reasons.

First, it is unclear whether consent as currently obtained from consumers is truly knowing and voluntary. Almost all data aggregators serve as third party intermediaries to the actual data user. When consumers clicking "I agree" to allow access to aggregators access, many do not truly 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 are not fully aware that apps or third parties may store their deposit account username and password, and more than 80% are not aware that apps may use third parties to access consumers' financial information.[7] The primary author of these comments – an experienced

[6] 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.").

[7] 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,

consumer attorney – was surprised to learn at the CFPB's Symposium on Section 1033 that she had authorized a data aggregator to access her account when she signed up for Venmo. If she did not understand when she clicked "I agree," what chance does the average consumer have?

Second, 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. A consumer's deposit account contains 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.

Third, even if the consumer is completely aware they are consenting to access by an aggregator, this 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 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, the CFPB should not forget that consent is not actually required by any statutory scheme, even Gramm-Leach-Bliley, 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, with the proposed project discussed in Section A.3 using EWS data, we can imagine more banks reporting account transaction data to that CRA without their customers' meaningful consent.

2. Strong rules are needed to ensure consumers retain control and their privacy is respected

To avoid the risks to consumer control, privacy, and misuse of their data, we urge the CFPB to adopt the following limitations as part of its Section 1033 rulemaking. These limitations are substantive in nature. As drafted by the CFPB, Questions 25 through 28 focus on "improving consumer understanding," suggesting that the Bureau is contemplating improved disclosures. But as the history of consumer protection demonstrates over and over again, the CFPB cannot rely on disclosures alone to protect consumers. Disclosures are a *necessary* component of a strong consumer protection regime, but they are never a *sufficient* measure standing alone.

---

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 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. While the use of deidentified data for research purposes might be the only exception to this limitation, we have serious concerns about the potential of re-identification that must first be addressed.

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. There is too great a risk that creditors and other users will require use of deposit account transaction data for all consumers, including those who could have received credit or other services 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 deposit account information. Expansion of consumer data to include deposit account information may benefit those consumers who have insufficient credit history information or lower credit scores due to past problems that have eased, but use of this data could hurt or risk the privacy of consumers who already qualify for mainstream credit.
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. Simply listing the name of aggregator is insufficient, as consumers might assume that the aggregator merely is a software provider. The role of the aggregator must be disclosed in a manner that consumers realize they are 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 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 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.

3. The CFPB has authority under Section 1033 and other laws in its jurisdiction to adopt strong limitations

The CFPB must adopt rules under Section 1033 or other statutory authority to adopt the limits described above. With respect to aggregators, the primary argument for allowing data aggregators access to account data is that they are an "agent" of the consumer (see Question 17 which acknowledges that argument). The CFPB must require in the Section 1033 rulemaking that an aggregator will only be considered the consumer's "agent" if the above limitations that are applicable to aggregators and data holders apply.

There is strong precedent for requiring that aggregators look out for the best interests of the consumer if they are to be considered an "agent." At common law, an agent acts on behalf of a principal, has a fiduciary relationship to that principal,[8] and is prohibited from using the principal's confidential information for its own benefit.[9] These above proposed limitations make sense in that context. Imagine if an attorney or realtor sold the consumer's data for uses that the consumer had not expected or knowingly authorized, or continued to access the data years after the legal case or home sale for which they had been retained? Surely that would be seen as a breach of their fiduciary agency relationship.

As for data users, the CFPB should adopt limitations 1, 2 and 3 above, as well as additional protections discussed below, under its authority pursuant to applicable laws (FCRA for credit and other covered uses; EFTA for payments; GLBA or UDAAP for other uses not covered by these Acts).

[8] Restatement (Third) Of Agency § 8.01 (2006) ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship").

[9] *Id.* at § 8.05 ("An agent has a duty … (2) not to use or communicate confidential information of the principal for the agent's own purposes or those of a third party.)

C. Data Security and Standardization

Data security is obviously critical in any system that accesses or uses consumers' 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"). More recently, 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, at least from the participants of the CFPB's 1033 Symposium, that data aggregation should move away from screening scraping and toward APIs. We, as well as Consumer Reports, support these efforts to increase the use of APIs and eliminate screen scraping, and consumer groups have been participating in the Financial Data Exchange (FDX), an initiative to set standards for APIs.

The CFPB should support and encourage efforts to move away from screen scraping. But the Bureau should not prohibit screen scraping 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 data holders the upper hand and ability to prematurely shut out access.

2. The CFPB should prescribe general "data dictionary" standards to ensure a common language and understanding (Question 15)

The CFPB has asked whether it should prescribe standards to promote the development of standardized formats for data authorized pursuant to Section 1033. The answer is clearly yes, because Section 1033 specifically requires it. Subsection 1033(d) specifically directs the CFPB to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files,…"

Stakeholders have urged the CFPB not to favor one platform or technology. While we can see why the CFPB would not want to favor one particular API or platform, the Bureau should still set or require general technical standards for consumer-authorized data. During the Symposium, stakeholders noted problems created by the lack of common technical standards.[10]

[10] *See, e.g.,* Written Statement of Jason Gross, Petal Card, Inc., CFPB Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, February 12, 2020 (" Without a common standard, current inefficiencies in data aggregation—including poor data reliability and expensive middlemen, among others—will proliferate, frustrating the will of consumers in accessing and porting their data, and contributing to an overall data lock-in effect, stifling portability despite what consumers want. Financial institutions should be required to maintain standardized APIs, and financial applications should have the ability to plug in directly if they so choose, using a common technical standard.")

One type of standardization that is critically important is a common data dictionary. For all their faults, this is an area where the nationwide CRAs have engaged in useful efforts to set a common data format, *i.e.*, the Metro 2 reporting format, that helps prevent disparities and ensures that all participants in a system are speaking a common language. The CFPB should develop its own common format or encourage the development of one industry-wide.

3. Data Security

Data security is obviously critical in any system that accesses or uses consumers' account data. Screen scraping is less than optimal from a data security perspective; this is another reason the CFPB should support and encourage efforts to move away from screen scraping.

In terms of regulatory regimes, CRAs are subject to the Federal Trade Commission's Safeguards Rule, promulgated pursuant to the Gramm-Leach-Bliley Act and currently the subject of a rulemaking to strengthen its requirements.[11] This is another reason why coverage of data aggregators as CRAs would be helpful when appropriate, a topic discussed in Section D.3 below. If an aggregator is not covered under the FCRA as a CRA, it is still likely that GLBA applies to them, but the CFPB should recommend to the FTC that it make explicitly clear that data aggregators are included in the scope of its Safeguards Rule.

As part of the CFPB supervision we advocate for in Section D.4, 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 CRAs for data security.

D. Legal Requirements Other than Section 1033 (Questions 33 to 37)

The CFPB has asked whether "regulatory uncertainty" due to the applicability of other laws is creating tension with Section 1033 or impeding competition or innovation. First, we question the underlying assumptions of this language, that there is significant uncertainty or that application of existing laws is 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. The comments of Consumer Reports provide several compelling examples of this subterfuge.

Moreover, the CFPB's core mission is consumer protection, not resolving "uncertainty" for new business models. So-called uncertainty often arises when companies seek to avoid older

[11] 84 Fed. Reg. 13158 (Apr. 4, 2019).

consumer protection laws. Resolving that uncertainty in ways that result in less protection for consumers does not fulfill the CFPB's purposes.

It is clear that certain existing laws apply in the context of consumer authorized access. If used for credit underwriting, the Fair Credit Reporting Act (FCRA) applies and the Equal Credit Opportunity (ECOA) is implicated. Because deposit accounts are involved, the Electronic Funds Transfer Act (EFTA) applies. And since financial information is involved, the Gramm Leach Bliley Act (GLBA) is implicated (discussed in Section C.3 above on data security). In some cases, there may be clarifications or small adjustments needed to address the application of these laws, but for the most part they are broadly and flexibly written and have stood up well over time.

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 the CFPB well knows, many consumers live paycheck to paycheck, with 40% of Americans who would struggle with an unexpected $400 bill.[12] 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.

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, data aggregator and data user. The consumers' right to contest unauthorized charges and to dispute error directly through their financial institution must be respected.

There are three different situations where more clarity or amendments to Regulation E or the official staff commentary may be warranted.

(a) Data breach at data aggregator or data user resulting in unauthorized charge

It is not difficult to envision the possibility that there could be a data breach at a data aggregator or a data user that results in the consumer's login credentials or account and routing number being stolen. Financial institutions are right to be concerned about the security of consumers' data and to insist that data aggregators access and hold data in a secure fashion.

But concerns about security should not be used to justify depriving consumers of their Regulation E rights to dispute unauthorized charges. In the past, some financial institutions

[12] 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.

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.

The definition of "unauthorized charge" in Regulation E excludes an electronic fund transfer initiated "**By** a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized."[13] That exception does not apply if the unauthorized charge was initiated by someone other than the person furnished the access device. For example, if the consumer gives their debit card to their teenage son and tells him he can spend $60 on a pair of shoes and instead he spends $200, the charge is not unauthorized. But if the son is mugged and the debit card is stolen, the consumer can contest unauthorized charges by the mugger.

Recommendation: We believe that Regulation E is clear on this point. But it would be helpful if the CFPB would emphasize to financial institutions that the exception for persons furnished the access device does not apply to unauthorized charges that are the result of a data breach.

This is not only the clear interpretation of Regulation E, but it also makes sense from a policy perspective. 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.

(b) Unauthorized charge by the data user

A second situation could involve an unauthorized charge as a result of an electronic fund transfer initiated by a data user (or, less likely, data aggregator[14]). For example, the provider of a mobile app that uses a data aggregator, and that enables the consumer to initiate transfers, could itself make an unauthorized transfer.

The account-holding institution might try to argue that the consumer has furnished an "access device" to the data user and thus the charge falls outside the definition of unauthorized charge.[15] However, the transfer initiated by the data user is unlikely to be through the consumer's access device to the account. Thus, the exclusion from the definition of unauthorized transfer would not apply.

[13] 12 C.F.R. § 1005.2(m)(1).

[14] Data aggregators do not typically initiate electronic fund transfers, and thus would be unlikely to make an unauthorized charge. They do, however, hold account information that could be subject to a data breach and result in an unauthorized charge, as discussed in the prior section.

[15] 12 C.F.R. § 1005.2(m)(1).

Even if login credentials, or a bank account and routing number, could be viewed as an access device in some situations, which is not clear, a reading of "access device" in the context of the unauthorized charge exception that is too expansive would swallow the protection against unauthorized charges. A consumer certainly does not lose protection any time they give a merchant or website a debit card, debit card number, or bank account and routing number. If a consumer enters her account information on a website, that does not deprive her of the ability to contest unauthorized charges by that website. The consumer can reach out to the merchant to address the unauthorized charge. But if they are unresponsive, the consumer still has the right contest the charge with the bank. The situation is no different with a mobile app or other data user that uses a data aggregator.

The exception in Regulation E for persons furnished the access device was designed for the situation where the consumer literally hands over a physical debit or ATM card to a friend or family member who then uses it at a store or ATM. The exception was not aimed at situations where the consumer enters their account information on a website or mobile app.

There is also a fundamental difference in the two situations: In the family member situation, if the bank were to reverse the charge, the merchant is innocent and would suffer the loss. In the data user situation, the user is the guilty party in that it was responsible for making the unauthorized charge, and there would be no injustice in reversing the charge.

Recommendation: Through guidance or other statements make clear that the "furnished the access device" exception to the definition of "unauthorized charge" in 12 C.F.R. § 1005.2(m)(1) does not apply to a consumer who supplies a data user with credentials necessary to enable use of data aggregation.

(c) Service providers that do not have an agreement with the account-holding institution

A third situation involves the application of the "service provider" provisions of Regulation E, 12 C.F.R. § 1005.14. The current application of those provisions, written in 1980, is unclear.

Separate from the definition of "financial institution," Regulation E has special "service provider" rules stating that "a person that provides an electronic fund transfer service to consumer but that does not hold the consumer's account" is nonetheless subject to all of the requirements of Part A of Regulation E (with some adjustments) if two conditions are met: the service provider:

> (1) issues an access device that the consumer can use to access an account held by a financial institution, and

(2) has no agreement with the institution that holds the account regarding that access.[16]

The official interpretations give the example that the EFTA can apply to an institution issuing a code for initiating telephone transfers that are to be carried out through the ACH system from a consumer's account at another institution.[17]

EFT service providers that do not hold consumer accounts are subject to special rules that include minor adjustments to the disclosure, documentation, and error resolution provisions of Regulation E.[18]

The duties of service providers is not problematic, but Regulation E also states that account-holding financial institutions need not comply with the requirements of Regulation E with respect to electronic fund transfers initiated through the service provider, except in connection with periodic statements; providing information or copies of documents needed by the service provider to investigate errors or to furnish copies of documents to the consumer; and honoring of debits following reversal of a provisional credit.[19]

This exception limiting the duties of the account-holding institution is not in the EFTA itself. The EFTA contains no exceptions to the account-holding institution's duty to comply with the error resolution, consumer liability or other provisions.

It is unclear to what, if any, situations these service provider provisions apply today. The service provider provisions of Regulation E were proposed in 1979[20] and finalized in 1980,[21] in the early days of electronic banking. Apart from minor changes,[22] the service provider provisions have not been significantly updated since then, and the CFPB has not given attention to how these older provisions apply to modern electronic fund transfer services.[23]

Even if the account-holding financial institution has an agreement with a data aggregator allowing access through an API, the institution is unlikely to have an agreement with the data users that are the customers of the data aggregator, though possibly there is an indirect agreement through the terms of the data aggregation agreement.

Most data users today that use data aggregators today do not provide the consumer with an access device, so the service provider rules would not apply. But that may change.

---

16 Reg. E, 12 C.F.R. § 1005.1]. *See* Reg. E., Official Interpretations § 1005.14.
17 Reg. E., Reg. E, Official Staff Interpretations § 1005.14.
18 12 C.F.R. § 1005.14 .
19 Reg. E, 12 C.F.R. § 1005.14(c).
20 44 Fed.Reg. 25850 (May 3, 1979); 44 Fed.Reg. 59464 (Oct. 15, 1979). The provisions were originally proposed as 12 C.F.R. § 205.4(b) but were later codified as 12 C.F.R. § 205.14 (which in turn was redesignated by the CFPB as 12 C.F.R. § 1005.14).
21 45 Fed.Reg. 8248 (Feb. 6, 1980).
22 *See* 52 Fed. Reg. 30904 (Aug. 18, 1987).
23 *See, e.g,* Jonice Gray Tucker, et.al, Square Peg Meets Round Hole: Regulatory Responses to Challenges Created By Innovation In Banking, 75 Bus. Lawyer 2491, 2499-2501 (Fall 2020).

Even if the service provider does supply an access device, it would be an untenable situation to relieve the account-holding institution of its error resolution duties (beyond the limited duty to provide information to the service provider or the consumer). The most obvious place for the consumer to turn if there are errors or unauthorized charges on their account is to the account-holding institution. Certainly the service provider should also have responsibilities, and should potentially bear the liability for any errors. But consumers should not be given the run-around or be deprived of the ability to contest unauthorized charges.

Recommendation: Regulation E section 1005.14 should be amended to reinstate the account-holding institution's duty to comply with Regulation E, while also requiring the service provider to cooperate with and potentially to reimburse the account-holding institution.

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. Consumer-authorized deposit account data will almost certainly 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.[24]

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.[25] 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, as Consumer Reports' comments discuss further. There is an assumption that algorithms are automatically unbiased or judgment free, but recent research indicates otherwise.[26] Recent studies and news reports have shown that computers can discriminate too, from digital mortgages[27] to Apple credit cards.[28]

---

[24] 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).

[25] 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.").

[26] *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

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.

The CFPB should ensure that the use of consumers' account data does not result in undue discriminatory impacts against consumers in any context. The Bureau should examine aggregators and lenders that it supervises to determine if the use of account data results in any disparate impacts. The CFPB should engage in continuing research that compares racial and protected class disparities in consumer-authorized data with corresponding disparities in credit scores and other traditional data sources.

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 "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 (ChexSystems, EWS). These terms also apply to new technology companies, including as data aggregators that provide third party information used for credit underwriting or other FCRA covered purposes.

Even the CFPB Taskforce on Federal Consumer Financial Law recognized that the FCRA applies when authorized data is used for credit decisions, one of the handful of pro-consumer

---

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.").

[27] *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).

[28] *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.

conclusions in its January 5, 2021 report.[29] Further analysis as to why the FCRA applies to data aggregators supplying information for FCRA-covered purposes (credit, employment, insurance, government benefits, etc.) is set forth in NCLC's Written Statement to the CFPB's 1033 Symposium in February 2020, attached and incorporated by reference. The remainder of this section discusses why the CFPB should not carve out an exclusion from the FCRA for aggregators that sell or share information that will be used for FCRA-covered purposes.

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:

- *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" notices 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). The CFPB has recognized the importance of accuracy and dispute rights as part of its seventh principle in the CFPB's *2017 Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*. These FCRA rights must be preserved when consumer-authorized account data is used for credit or other FCRA-covered purposes.

Some commentators have argued that, with respect to data aggregators, a data holder is not a "furnisher" under the FCRA.[30] That may make sense when the aggregator pulls the data from

[29] CFPB, Taskforce on Federal Consumer Financial Law Report, January 5, 2021, at Volume 2, p. 7, https://files.consumerfinance.gov/f/documents/cfpb_taskforce-federal-consumer-financial-law_report-volume-2_2021-01.pdf.

[30] Kwamina Williford and Brian Goodrich, Holland & Knight, Why Data Sources Aren't Furnishers Under Credit Report Regs, https://www.hklaw.com/-/media/files/insights/publications/2019/09/whydatasourcesarentfurnishersundercreditreportregs.pdf?la=en (visited January 29, 2021).

the holder without its permission or cooperation as in the case of screen scraping. A more complicated analysis is necessary when the data holder agrees to *permit* an aggregator to pull the data. Excluding data holders as furnishers under these circumstances could raise troubling risks. Creditors that currently furnish information to the nationwide CRAs or banks that furnish to ChexSystems/EWS might attempt to avoid the furnisher duties under 15 U.S.C. 1681s-2 by entering into bilateral agreements with the CRAs permitting the CRAs to pull account histories, seriously undermining the furnisher protections of the FCRA. The CFPB must guard against that possibility in any Section 1033 rulemaking. One possibility is that – *only when data is shared pursuant to the strong consumer controls as we advocate for in Section B.2* – could the data holder be considered to be a passive entity and not a furnisher, or its duties as a furnisher be limited. Pro forma authorizations buried in stacks of paperwork should never be sufficient for this purpose.

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 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, the CFPB could address this in its Section 1033 rulemaking by requiring data holders who are not furnishers to assist aggregators in processing disputes under the FCRA.

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 consumer-authorized 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.[31] To the extent that data from an aggregator is never used for an FCRA-covered purpose and is never part of a consumer report, we agree with the comments of Consumer Reports that 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

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

is preferable because it is a time-proven statute with an established body of law and clear, enforceable consumer rights.

4. Data aggregators should be subject to CFPB Supervision

As discussed through these comments, 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 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.

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,[32] as material service providers,[33] or as providers of a product or service that will likely have a material impact on consumers.[34] If the data aggregator is a CRA, it may already be a larger participant in the consumer reporting market and should be examined.

E. Other types of data (Question 18)

The CFPB's ANPR, as well as most of the stakeholder focus on a Section 1033 rulemaking, has been on authorized access to a consumer's deposit account information. However, Section 1033 potentially applies to other types of data "in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person." We urge the Bureau to use this authority to give consumers the right to several other types of information, including:

- a copy of the consumer report or risk score that a lender or other covered person used in connection with providing the consumer a financial product or service;
- records retained by a covered person pursuant to Regulation Z or Regulation B; and
- behavioral data sold by the nationwide CRAs to covered persons for marketing purposes, which the CRAs claim is not a consumer report and thus do not make available to consumers.

1. Copy of the consumer report used by the lender or other covered person

Under the FCRA, consumers are entitled a copy of their consumer report, *inter alia*, after a user takes an adverse action against them based on their report. 15 U.S.C. § 1681j(b). However, they must seek the consumer report from the CRA, which may provide a very different report than

[32] 12 U.S.C. § 5481(15)(A)((ix).
[33] 12 U.S.C. § 5481(26).
[34] 12 U.S.C. § 5481(15)(A)(x).

the report provided to the user.[35] In the worst-case scenario, the user report can reflect serious errors (such as mixed files, *i.e.* files that mix the information of two different consumers) that do not appear on the report provided to the consumer.[36] Consumers should be entitled to the user version of the report from users who are covered persons under Section 1033.

As for risk and financial scores, while the FCRA mandates a free disclosure of a credit score used by the user if there is an adverse action or risk-based pricing, this disclosure is limited to scores used to "predict the likelihood of certain credit behaviors, including default." 15 U.S.C. § 1681g(f)(2)(A)(i). The right to a free disclosure does not apply to other types of risk scores derived from consumer reports and used for consumer financial services or products, such as those used for marketing (*e.g.,* Experian's Mosaic Score) or debt collection activities. We urge the Bureau to consider using Section 1033 to provide to consumers with access to other risk scores used for financial products and services in the control or possession of covered persons.

2. Records retained pursuant to Regulation Z or Regulation B

Both Regulation Z, 12 C.F.R. § 1026.25(a), and Regulation B, 12 C.F.R. § 1002.12(b), require creditors to retain records as evidence of their compliance with, respectively, the Truth in Lending Act and the ECOA, for two years. Yet we have heard complaints from consumer attorneys that their clients are unable to access these records due to lack of cooperation by creditors. The CFPB should require that creditors provide access to these records pursuant to Section 1033.

3. Behavioral data

The nationwide CRAs have begun to sell behavioral data to lenders and other users for marketing purposes. For example, Experian sells ConsumerView, a product that provides "thousands of attributes on more than 300 million consumers and 126 million households" that "reveal demographics, purchasing habits, lifestyles, interests and attitudes."[37] It includes financial data as Experian describes:

> **Property and mortgage data** is perfect for marketers looking to reach consumers with real estate, refinancing or second mortgage offers. This data also is extremely indicative of the day-to-day financial responsibilities for households. With data compiled from public records and county deeds, you can reach consumers with offers based on reliable and up-to-date data.

[35] See National Consumer Law Center, Fair Credit Reporting § 3.7.2.2 (9th ed. 2017), updated at www.nclc.org/library.
[36] *Id.*
[37] Experian, ConsumerView brochure, Feb. 2018, https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/brochures/consumerview-brochure.pdf.

> **Financial data** segments go beyond income and estimate the way your customers spend their money. From Financial Personalities® that help outline consumer spending behavior to ConsumerView Profitability Score, which ranks households most likely to pay their debts, you can gain a 360-degree view of your customers' estimated financial habits.[38]

Despite the fact that the ConsumerView database appears to contain some important and sensitive financial information about consumers, Experian does not make file disclosures available to consumers about the product, and in fact has actively resisted doing so. *See* Tailford v. Experian Info. Sols., Inc., 2020 WL 2464797, at *6 (C.D. Cal. May 12, 2020) (dismissing claim that Experian was required to make file disclosures from ConsumerView database under 15 U.S.C. § 1681g).

If consumers cannot access the information about themselves in the Experian ConsumerView database, they should be entitled to access any information in the control or possession of covered persons who have accessed that information. The CFPB should require that consumers have access to this information under Section 1033.

* * *

Thank you for the opportunity to submit these comments and for your work to ensure consumers' ability to safely and easily access and use their financial account data. If you have questions about these comments, please contact Chi Chi Wu at cwu@nclc.org or 617-542-8010.

Respectfully submitted,

National Consumers Law Center
(on behalf of its low-income clients)
Americans for Financial Reform Education Fund
Center for Responsible Lending
Consumer Action
Consumer Federation of America
USPIRG

[38] *Id.*