



March 15, 2019

United States Senate
Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510
(submitted via email to submissions@banking.senate.gov)

Re: Feedback on the collection, use and protection of sensitive information by financial regulators and private companies

Dear Chairman Crapo and Ranking Member Brown:

Consumer Reports¹ appreciates the opportunity to provide feedback on the collection, use and protection of sensitive information by financial regulators and private companies. In the early 2000s, Consumer Reports worked around the nation to pass state laws establishing basic consumer protections against unauthorized disclosure of consumer data.² Since then, every state³ and more recently, Congress, has passed a law giving consumers the right to a security freeze.⁴ Every state has passed a data breach notification law to outline when and how companies must notify consumers when their information is compromised.⁵ Despite these advances, consumers remain more vulnerable to identity theft and other privacy harms than ever, as companies expand their data collection practices and find new ways to monetize consumer data.

¹ Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumer Reports works for pro-consumer policies in the areas of financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, telecommunications and technology, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

² *The Fair Credit and Identity Theft Protection Act: Model State Law*, CONSUMERS UNION OF U.S., INC. & THE STATE PUBLIC INTEREST RESEARCH GROUPS, Gail Hillebrand, Michelle Jun, & Ed Mierzwinski, eds. (Updated Jan. 2011), <https://advocacy.consumerreports.org/wp-content/uploads/2013/02/model.pdf>.

³ See *Consumer Report Security Freeze State Laws*, NAT'L CONF. OF STATE LEGISLATURES (June 26, 2018), <http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx>.

⁴ S. 2155 (2018), available at <https://www.congress.gov/bill/115th-congress/senate-bill/2155>.

⁵ See *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Mar. 29, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

It is time not only for providers to adopt best practices, but also for Congress to act. Congress should pass strong laws to incentivize companies to keep consumer data safe and provide consumers real privacy protection. In the event of a data breach, consumers should be notified promptly so that they can take appropriate remedial action, but a federal data breach notification law should only establish a high federal floor, not preempt stronger state laws. Congress should pass strong legislation to ensure the accuracy and integrity of consumer credit files. Federal regulators should be given the tools to hold companies accountable if they fall short in their obligations to consumers.

1. What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?

Consumers must have access to information about and the ability to control what information is collected, inferred and shared about them. Companies should only collect the information that is necessary for the purposes for which consumers have come to them. Companies should employ reasonable measures to keep consumer data secure, and all user information should be deleted after users terminate their account or remove service from a device. These best practices and more are outlined in The Digital Standard, an open-source digital privacy and security standard,⁶ which companies should adopt.

However, industry best practices are not enough. Consumer Reports urges Congress adopt national privacy legislation that contains:

- **Clear information about data practices.** Privacy policies today are often vague and inscrutable. Even if you take the time to read one in full, you probably still won't know what the company actually does with your data. This is because current law mostly allows companies to describe their data practices however they want and generally holds companies responsible only if they actively lie to consumers about what they do. And as a result, companies write very broad and confusing privacy policies that intentionally leave the door open to a wide range of business practices. That has to change. Companies should be required to clearly and accurately disclose their data practices—both in detailed legal notices and in a form that busy consumers can easily access, understand, and use for comparison. The law should require that these disclosures be standardized. Such information would also help organizations like Consumer Reports evaluate company practices and pass the analysis on to consumers.
- **Simple and easy-to-use consumer choices.** Some data collection is necessary just for a product to work. But a lot of practices are extraneous to the core functionality of a product—for example, the sale of information to third-party data brokers, or all-

⁶ *The Standard*, The Digital Standard, <https://www.thedigitalstandard.org/the-standard> (last visited Feb. 28, 2019).

encompassing surveillance of how consumers use a product in the name of “analytics” or “product improvement.” Consumers deserve easy, standardized tools that give them control over their information and allow them to stop companies from using their data for these extraneous purposes. Wherever possible, consumers should be able to make choices about multiple companies at once. For example, Consumer Reports supports the notion of a robust Do Not Track option in browsers to enable consumers to limit online tracking as they navigate the web.

- **The collection and retention of only the data necessary—and the disposal of old data.** Consumers shouldn’t bear the entire burden of protecting their privacy through settings and controls. Some practices should simply be out-of-bounds, because of the sensitivity of the data, or the potential for discrimination or abuse. What kind of information should be off-limits? One example might be details of a medical condition, revealed through a consumer’s web searches and online reading. Companies should also collect just as much data as they need to make their product or service work properly. For instance, a navigation app needs to know where you are, and where you want to go, but it probably doesn’t need access to your contacts. Next, companies should get rid of data they no longer need—today, many companies keep consumer information around indefinitely with the vague hope that they’ll be able to find new ways to exploit it later. But that poses a threat to consumers. Personal information left for years on corporate servers can be compromised in a data breach, put to unwelcome uses, included in a corporate sale, or accessed by others in litigation.
- **Strong data security practices.** Companies that collect and maintain personal information should put in place basic protections to ensure that outside attackers cannot access it. Last year’s Equifax breach highlights the urgent need for these protections—in that case, sensitive data on nearly 150 million people was stolen by criminal hackers because the company failed to keep its software updated. And many Internet of Things devices are being designed without even the most rudimentary security protections. If companies collect our information, they should be required to protect it.
- **Ways for consumers to get easy access to their information.** Consumers should be able to see what information companies maintain about them. Such access rights are a fundamental part of privacy laws in Europe and elsewhere. And in fact, overseas regulations have led to some companies making more information available to their American users as well. But those companies are the exception instead of the rule, and U.S. citizens shouldn’t have to rely on other countries to protect them. Additionally, services such as social networks should be required to make it easy for consumers to export their data, in case they want to switch services.

- **Strong enforcement tools to ensure accountability.** Even a strong privacy law won't help consumers unless it's backed up by strong enforcement. For more than 20 years, the FTC has taken the lead on privacy and security issues, but it has limited authority and inadequate resources. Specifically, the agency lacks two key tools: the power to obtain civil penalties for wrongdoing and the power to enact regulations clarifying what companies can and can't do with consumer data. Further, the FTC needs more staff on the consumer data beat, including technologists and computer scientists who can keep pace with Silicon Valley's race to collect and monetize more consumer information.⁷

Incentives to protect consumer data from unauthorized disclosure remain inadequate. For example, the Equifax data breach of 2017 led to the disclosure of the personal information, including Social Security numbers, of over 145 million Americans—about half of the United States population—leaving them susceptible to identity thieves seeking to open credit in their names for years to come.⁸ While credit bureaus like Equifax are required under the Gramm-Leach-Bliley Act and the Safeguards Rule to keep consumer data secure,⁹ the legislation provides no penalties for failure to comply.¹⁰ The breadth and depth of personal information involved could all-too readily also be used to defraud and otherwise manipulate the individuals affected.¹¹

Congress should pass strong data security requirements, with tough penalties for violations. First and foremost, Congress should require companies to implement reasonable data security procedures to protect consumer information. For years, Congress has failed to establish across-the-board, baseline requirements for data security, and consumers have paid the price. The law should cover not just Social Security numbers or financial account information but any information that, if breached, could put consumers at risk. Congress should also empower the FTC to develop rules to implement these requirements, in order to give greater clarity to companies covered by the law, and allow for updated standards as threats evolve. And to ensure sufficient and appropriate enforcement, state attorneys general should be able to enforce the new law, and there should be a private right of action, with a ban on mandatory arbitration provisions.

As part of the new law, Congress should include provisions to limit the harms caused by the overuse of Social Security numbers (SSNs). SSNs are too frequently compromised in high profile incidents, such as the recent Equifax and Office of Personnel Management breaches. Overuse of SSNs in consumer transactions creates increased risk, and invites further attempted breaches. A number of states, including California and New York, have already passed laws

⁷ *Where We Stand: Congress Should Pass a Strong Privacy Law, Now*, CONSUMER REPORTS (Apr. 9, 2018), <https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/>.

⁸ Jeremy C. Owens, *The Equifax Data Breach, In One Chart*, Marketwatch (Sept. 10, 2018), <https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07>.

⁹ 15 U.S.C. § 6801(b); 16 C.F.R. § 314.1.

¹⁰ 15 U.S.C. § 6805(a)(7).

¹¹ Kelli B. Grant, *Your Next Worry After the Equifax Data Breach: Fake Tax Returns*, CNBC (Oct. 9, 2017), <https://www.cnbc.com/2017/09/18/your-next-worry-after-the-equifax-breach-fake-tax-returns.html>.

that prohibit public display of SSNs, including on identification cards, but Congress should extend these protections to every state. Similarly, all consumers should have the ability to protect their SSNs when doing their taxes. Disclosure of SSNs leaves consumers vulnerable to criminals who choose to submit a false tax return in the consumer's name and steal their tax refund. Only consumers in Florida, Georgia, and the District of Columbia, and those who are invited to do so by the IRS, may request an IRS Identity Protection PIN, a six-digit number used to confirm the consumer's identity, to help protect against this type of fraud. Congress should ensure that all consumers have the ability to do so.

Congress should also pass a federal data breach law to ensure that all consumers receive notice in the event of a breach. The new federal law should provide a consistent, minimum obligation to notify consumers if their sensitive personal information has been breached. This basic obligation should not preempt the states, which have led the nation's efforts on data breach notification, from passing or enforcing stronger laws to protect consumers. A number of states have updated their data breach notification bills in recent years to address new types of security threats—like photo-sharing and social media accounts, and biometrics. Broad preemption would have stopped them from creating these new protections to address new threats from technological developments. Indeed, if a federal law were to preempt more protective state laws, the new law would have the perverse effect of weakening the already too weak incentives for companies to safeguard personal data. Unfortunately, many of the data breach bills proposed in recent Congresses do just that. As noted above, a strong federal bill must cover all information that can be used to harm consumers and authorize civil penalties adequate for deterrence. Further, it should give the FTC rulemaking authority, authorize enforcement by the state attorneys general, and grant private rights of action, with no mandatory arbitration.

2. What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

In many areas of law, the backbone of consumer protection is disclosure. The idea behind requiring disclosures is that if companies provide consumers information, consumers can make an informed choice. For privacy protection, the idea is often referred to as “notice and consent”—consumers are given notice of a company's practices, and by clicking “agree” consumers “consent” to those practices. The problem with disclosure as a means of protecting consumer privacy is that the notices are useless to most because, as research shows, most consumers simply click “agree” without reading them.¹² Similarly, the disclosures required by the Gramm-Leach-Bliley Act, which are intended to give consumers the opportunity to opt-out of the sharing of nonpublic personal information with third parties and to outline the company's data

¹² Caroline Cakebread, *You're not alone, no one reads terms of service agreements*, Bus. Insider (Nov. 15, 2017), <https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11>.

use practices,¹³ are so confusing that consumers are unlikely to exercise their rights.¹⁴ Privacy Rights Clearinghouse found that these disclosures are typically written at a college level.¹⁵ While disclosures alone will not be adequate to ensure consumer understanding about data collection and use, as discussed in the following section, companies must be required to be transparent about their data collection, data security, and data sharing practices.

Adequate disclosures allow the few consumers who read them and the regulators and enforcement agents who rely on them to hold businesses accountable for their practices. Although lengthy disclosures at the initial point of interaction have not fostered sufficient consumer understanding—as noted above, few consumers read these policies—companies should still be required to provide these disclosures and be more transparent and explicit about their data collection and practices. While few consumers read privacy policies, detailed disclosures should be written for the groups that already read them: regulators, reporters, and consumer-protection organizations like Consumer Reports. All of these entities are engaged in monitoring privacy policies for policy, consumer protection, and investment purposes and should continue to do so, but with more explicit information at hand. Today’s policies are often vaguely expansive, providing little reliable concrete information about companies’ actual practices. A transparency mandate to provide more precise information could remedy that.

Requiring providers to draft and promulgate lengthy disclosures alone is not enough. There are things service providers and Congress can do. Companies should provide consumers with in-the-moment disclosures about how their data is being collected, used, and shared, and given the opportunity to opt out of data collection and sharing where appropriate. Before implementation, providers should test these disclosure methods to ensure consumer understanding. Congress should also act to enact privacy legislation that includes affirmative restrictions on financial institutions’ sharing of consumer data.

3. What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?

Consumers, as noted above, rarely read the documents that describe what information companies collect about them and with whom it is shared. Moreover, even if consumers do read these policies, they often encounter vague and sweeping language that is a barrier to meaningful notice and consent. Privacy by design, including data minimization, is critical. Financial services companies should collect and store only the information necessary for the

¹³ 15 U.S.C § 6802(b).

¹⁴ *Statement of Travis Plunkett, Legislative Director, Consumer Federation of America on Behalf of the Consumer Federation of America, Consumers Union, and the U.S. Public Interest Research Group, before the U.S. Senate Comm. on Banking, Housing, and Urban Affairs* (July 13, 2004), available at <https://www.govinfo.gov/content/pkg/CHRG-108shrg26700/html/CHRG-108shrg26700.htm>.

¹⁵ Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, Privacy Rights Clearinghouse (July 2001), <https://www.privacyrights.org/blog/lost-fine-print-readability-financial-privacy-notices-hochhauser>.

purposes for which consumers have sought them out. Consumers should have to opt-in for the sharing of their personal financial data and have the ability to revoke such access, and sharing should be done in line with reasonable consumer expectations.

The Consumer Financial Protection Bureau should continue to collect and analyze anonymized consumer financial information so it can fulfill its mission, and the Bureau should continue to make anonymized consumer complaint information, including narratives, available to the public.

4. What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?

Information collected by credit bureaus not only affects consumers' ability to obtain a mortgage, car loan, or credit card but can even be used to determine whether they can rent an apartment or get a new job. Consumers need robust protections to ensure that the information collected about them is accurate, accessible, and secure. The Equifax data breach, in which the personal information of nearly half of America was exposed, underscores the desperate need to reform credit bureaus. Despite the fact that the credit bureaus' business is built upon assembly of consumer data, typically without the knowledge or affirmative consent of the data subjects, individual consumers are not the credit bureaus' customers. Thus, it is very difficult for consumers to directly apply market forces to change industry behavior. As a result, it is critical that Congress act.

Persistent problems with the credit reporting process include "mixed files"—when another consumer's data is mistakenly in the credit file—and failure to thoroughly investigate an error dispute. Too often, credit bureaus simply pass error disputes on to furnishers, who may reconfirm existing information in their databases without conducting a thorough review. Therefore, we recommend that Congress impose new accuracy requirements on credit bureaus, such as matching requirements to ensure the right information is assigned to the right file. Congress should also require credit bureaus to forward to the furnisher—and require furnishers to thoroughly examine—all documentation provided by the consumer in the event of a dispute.

The credit reporting industry should also make it easier for consumers to access their own credit files and scores. Consumers are guaranteed a free credit report once a year from each of the three major credit bureaus. However, given the risks of identity theft that consumers now face, Congress should ensure that all consumers have access to more than one free credit report each year, and that specialty consumer reporting agencies are also required to provide free reports at no charge every year. Likewise, all consumers should be guaranteed access, for free, to a reliable credit score that is used by lenders when they access their free credit reports.

We also recommend that Congress consider taking additional steps to strengthen consumers' control over the use of their personal data by the credit bureaus. While free credit freezes are an important step, Congress should consider legislation to ensure that consumers understand what data is collected about them and how it is used. And it should consider taking the further step of

freezing consumer credit by default, enabling individuals to allow companies to access their credit report.¹⁶

Finally, Congress should consider barring credit bureaus and lenders from using certain data elements in the credit decision process due to significant concerns about disparate impact, transparency, privacy, and the predictive value of that data. For example, credit bureaus and lenders should not be permitted to use social media and web browsing data in deciding whether to grant credit. Not only could this reinforce inequalities in credit scoring along lines of race and ethnicity, but also it is unclear whether the data is predictive of a consumer's ability to repay.

5. What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

In 2017, the Consumer Financial Protection Bureau published Consumer Protection Principles: Consumer–Authorized Financial Data Sharing and Aggregation.¹⁷ These principles contain best practices for companies that access consumer financial account data (with consumers' authorization) and either use that information to provide products and services to consumers, or funnel that information to companies that do so. As the Bureau points out, while the promises of this data sharing are many, and include better underwriting and innovative financial management tools, it poses perils as well. We agree with the Bureau that consumer interests must be the priority of all stakeholders as the uses of and products built on data aggregation develop, and that the principles of transparency, access and control are critical. Congress should consider establishing consumer rights to correct these data and clear accountability of providers. We further suggest that consumers have the right to safely, quickly and easily port their data, and ideally their account numbers, from one service provider to another. This will ensure robust competition and prevent consumers from being “trapped” at a particular financial service provider.¹⁸

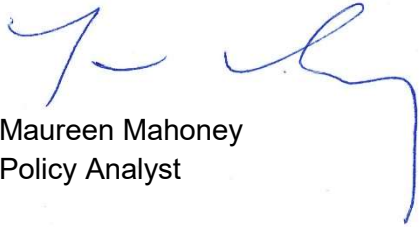
¹⁶ For more on this, and other credit reporting recommendations from Consumer Reports, see Letter from Consumer Reports to Chairwoman Maxine Waters, House Financial Services Committee (Feb. 26, 2019).

¹⁷ *Consumer Protection Principles*, Consumer Fin. Protection Bureau (Oct. 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

¹⁸ For more on ensuring consumer choice in banking, see *Trapped at the Bank: Removing Obstacles to Consumer Choice in Banking*, Consumer Reports (May 20, 2012), <https://advocacy.consumerreports.org/research/trapped-at-the-bank-removing-obstacles-to-consumer-choice-in-banking/>.

Thank you for the opportunity to comment. We look forward to working with the Committee on these important issues.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Maureen Mahoney', with a long horizontal stroke extending to the right.

Maureen Mahoney
Policy Analyst

A handwritten signature in blue ink, appearing to read 'Katie McInnis', with a long horizontal stroke extending to the right.

Katie McInnis
Policy Counsel

A handwritten signature in blue ink, appearing to read 'Christina Tetreault', with a long horizontal stroke extending to the right.

Christina Tetreault
Senior Policy Counsel