ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

October 2, 2017

United States Senate
Washington, D.C. 20510

Dear Senator,

Consumers Union, the policy and mobilization division of Consumer Reports,[1] writes to urge Congress to take long overdue action to protect the sensitive personal information of Americans. Last month, Equifax announced a monumental data breach affecting 143 million individuals. The breach exposed highly sensitive personal data—including Social Security numbers, driver's license numbers, and birth dates—and exploited a vulnerability that had been publicly announced several months earlier.[2] As a result of this breach, nearly half of the U.S. population is at risk of identity theft, potentially for the rest of their lives. Over 200,000 people have signed our petition asking Congress to take decisive action to hold Equifax accountable, and to provide stronger protections over their personal information.[3]

Although this is one of the largest breaches to date, it is hardly the first to put consumers' data at risk. Over the last 15 years, hundreds of companies ranging from high-end retailers to hotel chains, and from pharmacies to data brokers, have been compromised, with consumers bearing the brunt of the harm. And while breaches can occur even when companies take reasonable precautions, many breaches have been caused by companies' carelessness and lack of accountability. After years of failed bills and stalled debates, it is time for Congress to make data security a national priority, and to pass a law establishing these essential consumer protections:

- **Strong data security and data breach notification requirements for companies;**
- **Free security freezes, and better access to fraud alerts for consumers;**
- **Stronger controls over the sensitive data that credit bureaus collect and use.**

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of financial services, privacy and data security, auto and product safety, healthcare, and food safety, among many other areas. Using its more than 60 labs, auto test center, and survey research center, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.
[2] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX.COM (Sept. 15, 2017), https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/.
[3] *Congress Must Hold Equifax Accountable*, CONSUMERS UNION (Sept. 8, 2017), https://secure.consumersunion.org/site/SPageNavigator/20170908EquifaxPetitionPage.html;jsessionid=00000000.app223b?NONCE_TOKEN=9918995BF13130F7A53497A05E2E6FAC (last visited Sept. 28, 2017).

The failure to protect personal data causes real harm to consumers. Over 15 million U.S. consumers fell victim to identity theft in 2016, costing them $16 billion.[4] Victims spend precious time and money repairing the damage to their credit and accounts. Medical identity theft, in which thieves use personal information to obtain medical services, exhausts consumers' insurance benefits and leaves them with exorbitant bills. Tax identity theft occurs when thieves use consumers' Social Security numbers to obtain tax refunds. Fraudulent information on credit reports also causes consumers to pay more for a loan or be denied credit. And breaches take a toll on businesses too—in 2017, the average cost of a breach to companies globally was $3.62 million.[5] But despite these clear harms, little has been done at the federal level to ensure that companies protect sensitive consumer data. As a result, hackers continue to target vulnerable companies—year in and year out, and increasingly from overseas.

Without a clear regulatory framework for data security, Equifax and other companies across the marketplace have insufficient incentives to be better stewards of consumers' personal data. The market simply will not fix this problem—indeed, it was not until the states began enacting data breach laws in the early 2000s that companies even disclosed their breaches to the public. Although virtually all of the states have now passed these laws, few have *data security* laws, which are needed to prevent breaches from happening in the first place. And while the Federal Trade Commission (FTC) has taken many dozens of actions against companies that fail to protect consumer data, there are many gaps in its enforcement authority that put consumers at risk. In addition, even as many companies profit handsomely from using consumer data, they offer consumers little or no control over their data practices, and little or no recourse for data lapses.

Equifax is a prime example. Consumers have no say in whether their data is shared with Equifax, even though the company makes hundreds of millions in profits from consumer data every year.[6] Further, its reckless handling of the breach and its aftermath—including its delay in addressing a known vulnerability, delay in providing breach notices, meager remedies for consumers, inclusion of a forced arbitration provision, and rollout of a defective website—suggest that consumers rank very low on the company's list of priorities.[7] On September 14, Consumers Union wrote a letter to Equifax laying out seven steps it must take to make consumers whole: (1) free credit freezes at all the major credit bureaus; (2) free credit monitoring

---

[4] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, JAVELIN (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

[5] *Cost of Data Breach Study*, IBM (2017), *available at* https://www.ibm.com/security/data-breach/index.html.

[6] Equifax, Inc., Annual Report (Form 10-K), at 27 (Jan. 31, 2017), *available at* https://www.sec.gov/Archives/edgar/data/33185/000003318517000008/efx10k20161231.htm#sA091C585A07E5A24BBC2E110B9762C1A ($489 million in net income in 2016).

[7] While CEO Richard Smith was forced to step down after the breach, his $90 million severance package is unlikely to deter other executives from similar behavior. Jen Wieczner, *Equifax CEO Richard Smith Who Oversaw Breach to Collect $90 Million*, FORTUNE (Sept. 26, 2017), http://fortune.com/2017/09/26/equifax-ceo-richard-smith-net-worth/.

indefinitely; (3) more detail about the security incident; (4) no mandatory arbitration clauses; (5) sufficient staff to review and process disputes; (6) a fund to compensate injured consumers; and (7) an investigation of the three officials who sold stock just prior to the breach's announcement.[8] To date, Equifax's response to these requests has been negligible. It is time for Congress to protect consumers and give them greater control over their personal data.

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 baseline requirements for data security, and consumers have paid the price. Although there are laws currently on the books, they contain many gaps and impose few if any sanctions for noncompliance. Notably, the Gramm-Leach-Bliley Act requires reasonable data security for financial institutions, but does not apply to other types of companies or provide fines for violations.[9] The Fair Credit Reporting Act (FCRA) similarly requires credit bureaus to implement reasonable procedures to protect data, but is limited to that one industry and only applies to some of the databases the credit bureaus maintain.[10]

Outside these specific industries, the federal legal protections are even weaker. The FTC has used its general purpose consumer protection authority to take action against over 60 companies with lax data security practices.[11] However, the FTC lacks authority over banks, common carriers, and nonprofit entities, and generally cannot impose fines for violations.[12]

For example, in the FTC's cases against TJX, Reed Elsevier, and Uber, there were no fines or other financial sanctions.[13] Additionally, earlier this year, the FTC brought an action against D-Link, a company that manufactures webcams designed for the very purpose of helping consumers monitor and secure their homes. Despite the fact that there were several known security weaknesses in D-Link's security systems, making them vulnerable to takeover by malicious software, a judge ruled that to substantiate some of the charges, the FTC needed to

---

[8] Octavio Blanco, *Consumers Union Demands Equifax Make Affected Consumers Whole*, CONSUMER REPORTS (Sept. 14, 2017), https://www.consumerreports.org/equifax/consumers-union-demands-equifax-make-affected-consumers-whole/.

[9] Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[10] 15 U.S.C. § 1681. Equifax has said that its breach only affected certain databases, calling into question whether the FCRA applies.

[11] *See* Fed. Trade Comm'n, Data Security, https://www.ftc.gov/datasecurity.

[12] In addition, few states have passed data *security*, as opposed to data *breach*, laws.

[13] *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers Data*, FED. TRADE COMM'N (Mar. 27, 2008), https://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx; *Uber Settles FTC Allegation that It Made Deceptive Privacy and Data Security Claims*, FED. TRADE COMM'N (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.

show that consumers had been harmed, not just that D-Link's actions put consumers at risk.[14] However, in the event of a data breach, it is often difficult, if not impossible, to reliably attribute harm to a particular incident. Hackers do not typically disclose the source of the information they use to defraud consumers, and may wait for years to use it. And consumers who are harmed often have no way to trace the harm back to a particular company, or to a particular breach that may or may not have been announced.

Congress must address these problems by establishing strong federal data security requirements with tough civil penalties. The law should cover not just financial data 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 that prohibit public display of SSNs, including on ID cards, but Congress should extend these protections to every state.[15]

Similarly, all consumers should have the ability to protect their SSNs when doing their taxes. In 2016, the IRS intercepted nearly 1 million fraudulent tax returns, totaling $6.5 billion.[16] 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.[17] Congress should ensure that all consumers have the ability to do so.

---

[14] FTC v. D-Link Systems, Inc., No. 3:17-cv-00039-JD at 8-9 (N.D. Cal. Sept. 19, 2017) (order re: motion to dismiss), *available at* https://consumermediallc.files.wordpress.com/2017/09/dlinkdismissal.pdf.

[15] Consumers Union and the State Public Interest Groups, The Clean Credit and Identity Protection Act: Model State Law, 1-3 (Jan 2011), *available at* http://consumersunion.org/pdf/model.pdf.

[16] Written Testimony of John A. Koskinen Before the Senate Finance Committee on the 2017 Filing Season and IRS Operations, INTERNAL REVENUE SERV. (Apr. 6, 2017), *available at* https://www.irs.gov/newsroom/written-testimony-of-john-a-koskinen-before-the-senate-finance-committee-on-the-2017-filing-season-and-irs-operations-april-6-2017.

[17] Internal Revenue Serv., The Identity Protection PIN (IP PIN), (Oct. 1, 2017), https://www.irs.gov/identity-theft-fraud-scams/the-identity-protection-pin-ip-pin.

Strong data breach notification law, as a federal floor for consumer protections.

Congress should also pass a federal data breach law to ensure that all consumers receive notice in the event of a breach. Although data breach laws have been adopted in all but two states, these laws are inconsistent, and some offer insufficient protections. For example, many state laws have high thresholds for notice to consumers, or fail to define personal information broadly enough.

Consumers Union has a long history of advocating for strong data breach notification laws, including the first in the nation—California's, passed in 2002.[18] The premise of these laws is that an entity that has experienced a security breach should not get to decide whether or not to notify consumers about it. For consumers, notice of a data breach is necessary so that they can protect themselves from identity theft or other harms. These laws also provide incentives for companies and government agencies to take data protection seriously.

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. 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.

Free access to security freezes and better access to fraud alerts for consumers.

All 50 states and the District of Columbia now have laws on the books that permit consumers to place a security freeze on their credit reports with the major credit bureaus. Consumers Union played a key role in supporting the first one, enacted in California in 2001.[19] A security freeze gives consumers the choice to "freeze" or block access to their credit file against anyone trying to open up a new account or get new credit in their name.

As with data breach notification laws, the protections of the state security freeze laws vary. Not all states allow parents or guardians to place security freezes on a minor's credit reports, and most states allow credit bureaus to charge fees to place or lift a freeze. Moreover, no states that we are aware of provide consumers the right to place a freeze on their specialty

[18] *See* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.
[19] *See* https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200120020SB168.

consumer reports. Specialty consumer reports contain information on consumer's medical conditions, drug prescriptions, tenant history, employment, check writing, and insurance claims.

Consumers also face barriers in setting up fraud alerts. When a fraud alert has been included in a consumer's credit file, potential creditors must take an extra step to confirm the consumer's identity before extending credit. While fraud alerts are not as strong as security freezes, it should be easier for consumers to take advantage of that option if they choose. Under the FCRA, initial fraud alerts last a minimum of 90 days, at which point they may be renewed by the consumer. In addition, those requesting the alert must claim that they suspect that they are—or are about to be—a victim of fraud, such as identity theft.[20]

To address these problems, Congress should pass legislation that gives consumers easier access to security freezes and fraud alerts. Ideally, a federal security freeze law should:

- Ensure that consumers may not be charged for any security freeze services;
- Provide consumers an additional free credit report and a free credit score when placing a security freeze;
- Allow consumers to place freezes not only on reports and scores from credit reporting agencies but also on specialty consumer reports;
- Allow parents or guardians to place freezes on minors' reports;
- Clarify that all consumers may request an initial fraud alert, and extend the minimum period for an initial fraud alert for at least one year; and
- Authorize meaningful penalties for violations.

Stronger controls over the sensitive data that credit bureaus collect and use.

The Equifax breach illustrates the enormous range of information that credit bureaus collect about consumers—information that determines whether consumers get jobs, loans, insurance, phone service, cars, and many other services that are essential to daily life. To ensure that consumers are not denied these benefits based on flawed information, Congress should strengthen existing requirements governing credit report accuracy and fairness.

In particular, Congress should direct the Consumer Financial Protection Bureau (CFPB) to issue rules with more specific requirements for the credit bureaus and data furnishers, to make it easier for consumers to correct credit reporting errors. According to the FTC, about one in five consumers has a confirmed error on one or more of their reports from a major credit bureau.[21] Credit reporting is the third most-complained about topic to the CFPB, and over three-quarters of

[20] 15 U.S.C. § 1681c-1(a)(1).
[21] *In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports that Could Result in Less Favorable Terms for Loans*, FED. TRADE COMM'N (Feb. 11, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports.

those complaints are related to errors on a consumer's credit report.[22] Today, too many consumers suffer from errors and inaccuracies on their credit reports—many of them because they are victims of identity theft. The average victim of identity theft spends far too much time—an average of seven hours, but the process can sometimes take six months or more—addressing the resulting financial and credit problems.[23]

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.[24] 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.[25]

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.

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.[26] 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 it is unclear whether the data is predictive of a consumer's ability to repay.[27] Moreover, the chilling effect on free expression and free association is too great—consumers

---

[22] Consumer Fin. Prot. Bureau, Monthly Complaint Report, 5, 12 (Feb. 2017), *available at* https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201702_cfpb_Monthly-Complaint-Report.pdf.
[23] U.S. Dep't of Justice, Victims of Identity Theft, 2014 10 (Sept. 2015), *available at* https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[24] Consumer Fin. Prot. Bureau, Supervisory Highlights Consumer Reporting Special Edition, 10-11, 20-21 (Mar. 2017), *available at* http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.
[25] *See* Maureen Mahoney, *Errors and Gotchas: How Credit Report Errors and Unreliable Credit Scores Hurt Consumers*, CONSUMERS UNION (Apr. 9, 2014), http://consumersunion.org/wp-content/uploads/2014/04/Errors-and-Gotchas-report.pdf.
[26] *See Big Data: A Big Disappointment for Scoring Consumer Risk*, NAT'L CONSUMER LAW CTR. (Mar. 2014), *available at* https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.
[27] Robinson + Yu, *Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace* 21-22 (Oct. 2014), https://www.teamupturn.com/static/files/Knowing_the_Score_Oct_2014_v1_1.pdf.

should not be worried that the websites they browse and the people they connect with on social media will be used to determine their creditworthiness.

Conclusion

For too long, inadequate federal laws have allowed companies to collect and profit from the use of consumers' personal information, without consumers' knowledge or control, and without the incentives to properly steward that information and protect it from criminals. Given the unprecedented level of data collection in today's marketplace, and emergence of new privacy threats every day, now is the time to ensure that all Americans have the data protections they deserve. Consumers Union looks forward to working with members of Congress, in a bipartisan fashion, to address these vital consumer protection issues.

Sincerely,

Jessica Rich
Vice President, Policy and Mobilization

Justin Brookman, Director, Consumer Privacy and Technology Policy

Anna Laitin, Director, Financial Policy

Consumers Union
1101 17th Street, NW, Suite 500
Washington, DC 20036