ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

March 7, 2018

The Honorable Blaine Luetkemeyer, Chairman
The Honorable Carolyn Maloney
Subcommittee on Financial Institutions and Consumer Credit
United States House of Representatives
Washington, DC 20515

Dear Chairman Luetkemeyer and Representative Maloney:

Thank you for the opportunity to provide feedback on the recently-released draft data security and data breach legislation, the Data Acquisition and Technology Accountability and Security Act.[1] Data security plays an increasingly important role in consumers' everyday lives, and we strongly urge Congress to take action to update consumer protections to ensure that companies use reasonable precautions to protect sensitive personal information.

While we appreciate your leadership in this vital area, Consumers Union, the advocacy division of Consumer Reports,[2] has significant concerns about this bill and is strongly opposed to it in its current form. This bill would replace strong data protections in many states with a weaker set of criteria, including an unworkably high bar to trigger data breach notification requirements. Furthermore, this legislation would exempt Equifax, whose lax data security practices led to one of the largest data breaches in American history,[3] along with the other credit bureaus that collect and sell sensitive personal information about consumers. The bill's preemption provisions are so extreme that they would repeal and prohibit state laws that protect data not covered by this bill, such as online accounts and the Internet of Things. To better protect the privacy and security of consumers and businesses, Congress should pass legislation that sets strong baseline protections—with strong data security and notification requirements and substantial penalties for failure to comply—while allowing state protections to evolve over time to address an ever-changing array of threats.

The dramatic increase in data breaches in recent years highlights the need for stronger data security and data breach notification laws. Breaches at Equifax, the Office of Personnel Management,[4] and Target[5] seriously compromised the personal and sensitive information of hundreds of millions of Americans. Due to the Equifax breach alone, nearly half of Americans are now at immediate risk of new account fraud, and will be at risk for years to come. But there are many more breaches of which consumers may

[1] *See*, Data Acquisition and Technology Accountability and Security Act, Discussion Draft (Feb. 16, 2018), *available at* https://www.aba.com/Advocacy/Grassroots/WINNDocs/discussion-draft-data-acquisition-technology-accountability-security-act.pdf#_ga=2.88240539.1015636536.1518999145-1078425513.1518999145.

[2] Consumers Union is the public policy and advocacy division of Consumer Reports, an expert, independent, nonprofit organization whose mission is to work for a safe, fair and just marketplace for all consumers and to empower consumers to protect themselves. Consumers Union conducts its policy and advocacy work in the areas of telecommunications, healthcare, food and product safety, financial reform, and other areas.

[3] Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.

[4] Brendan I. Koerner, *Inside the Cyberattack that Shocked the US Government*, WIRED (Oct. 23, 2016), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[5] Kevin McCoy, *Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers*, USA TODAY (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/.

not be aware. In 2016, there were nearly 1,000 data security incidents involving financial institutions alone.[6] These breaches are costly for Americans: the following year, identity theft cost Americans nearly $17 billion.[7]

Data breaches are harmful for businesses, too, costing them an average of $3.62 million globally in 2017.[8] Summit Credit Union of Madison, Wisconsin recently testified that fraudulent charges related to data breaches cost them hundreds of thousands of dollars in 2017, not even counting the costs to replace credit and debit cards and for staff time to help resolve issues.[9] And as Javelin points out, "[D]ata breaches are causing consumers to lose trust in institutions[,]" as they increasingly feel that companies need to do a better job of securing their data.[10] Furthermore, about 18% of breaches involved state-affiliated actors[11] (and were responsible for over half of the breaches at educational institutions)[12] — suggesting that our national security is at stake as well.

Above all, any federal legislation must not simply replace existing state protections with a weaker federal standard but should instead affirmatively advance the state of data security in this country. Forty-eight states have data breach notification laws in place,[13] many of which have considerably stronger standards for notification than the draft legislation. Additionally, fifteen states have already passed data security laws requiring reasonable safeguards for personal information.[14] Replacing these protections with the rules in the Data Acquisition and Technology Accountability and Security Act would in many cases leave consumers *worse* off than they are today.

To improve this bill, we recommend the following changes:

- **Amend the bill to cover Equifax and other financial institutions:** As currently drafted, this bill would not apply to companies such as Equifax. As the Equifax breach demonstrated, these companies lack adequate data security regulations. Currently, they are covered by the Gramm-Leach-Bliley Safeguards Rule, which requires reasonable data security for financial institutions, but does not provide comprehensive breach notification requirements, or fines for violations.[15] As a first step, this bill should be expanded to cover these institutions.

- **Expand the scope of covered information beyond financial data:** Some states have revised their breach notification rules to include online accounts for email, photo storage, and social

[6] *2017 Data Breach Investigations Report*, 10th ed., VERIZON 19 (2017), http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ [hereinafter VERIZON DATA BREACH REPORT].
[7] *Identity Fraud Hits All Time High with 16.7 Million Victims in 2017, According to New Javelin Strategy & Research Study*, JAVELIN (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin [hereinafter JAVELIN STUDY].
[8] *Cost of Data Breach Study*, IBM (2017), *available at* https://www.ibm.com/security/data-breach/index.html.
[9] Written Testimony of Kim M. Sponem Before the House Fin. Svcs. Subcomm. on Fin. Institutions and Consumer Credit 2 (Feb. 14, 2018), *available at* https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-ksponem-20180214.pdf.
[10] JAVELIN STUDY, *supra* note 7.
[11] VERIZON DATA BREACH REPORT, *supra* note 6, at 3.
[12] *Id.* at 18.
[13] National Conference of State Legislatures, Security Breach Notification Laws (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[14] National Conference of State Legislatures, Data Security Laws—Private Sector (Dec. 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.
[15] Pub. L. No. 106-102, 113 Stat. 1338 (1999); 16 CFR 314.

media. These types of accounts often include incredibly sensitive information, and consumers should be told if those accounts are compromised. Similarly, data security requirements should be expanded beyond financial data. For example, many Internet of Things devices have infamously poor security, and yet these same devices are in our homes, enabled with cameras and microphones. Developers should be required to embed reasonable security protections in these devices, and other products and services that access sensitive—but non-financial—information. And the Federal Trade Commission should be empowered to amend the definition of personal information over time, as technologies and norms evolve.

- **Limit preemption:** This bill not only fails to address sensitive, non-financial data—it wholly preempts state laws that provide security or notification requirements for those types of data. We believe that a federal notification regime should set a floor not a ceiling on consumer rights, but certainly a federal statute should not broadly prohibit state laws from protecting categories of data not covered by a federal bill. The states have been leaders on enacting new protections to deal with evolving threats to personal security: this bill should not freeze protections in time, prohibiting the states from acting to protect their citizens to address future unknown threats.

- **Strengthen notification trigger to notify consumers unless reasonable belief sensitive information not acquired**: Companies should not be left to decide whether to inform consumers that their sensitive information has been affected. The current draft of the bill requires covered entities to notify only if they determine that the compromise of consumer data would create "reasonable risk that the breach has resulted in or will result in identity theft, fraud, or economic loss." Instead, companies should be held to a stronger notification standard: to alert the authorities immediately unless there is a reasonable assessment that sensitive data has not been compromised.

- **Require remediation:** Data breaches leave consumers vulnerable to identity theft. Affected consumers should be provided, at minimum, reimbursement for security freezes and access to free credit monitoring, with no mandatory arbitration clauses, as long as they remain susceptible to identity theft as a result of the breach.

- **Strengthen penalties:** Strong penalties provide important incentives for companies to adhere to data security requirements. Consumers should have the right to file suit against covered entities who fail to comply with the law, so that they are held accountable in appropriate cases even if federal and state authorities decline to take action.

The costs of indiscriminate data collection and data breaches to consumers, businesses, and the nation are too great to ignore. We look forward to working with you to ensure that Americans have the data security protections that they need.

Sincerely,

Justin Brookman
Director, Consumer Privacy and Technology
Consumers Union

Anna Laitin
Director, Financial Policy
Consumers Union

Cc: Members of the Subcommittee on Financial Institutions and Consumer Credit