March 14, 2019

The Honorable Mike Crapo
Chairman
Senate Committee on Banking
534 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member
Senate Committee on Banking
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

The Conference of State Bank Supervisors (CSBS) appreciates the opportunity to comment in response to your request for feedback on the collection, use and protection of sensitive information by financial regulators and private companies. We appreciate your bi-partisan efforts to address the very important issue of data security and data privacy.

CSBS is the nationwide organization of banking regulators from all 50 states, American Samoa, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. The mission of CSBS is to support the leadership role of state banking supervisors in advancing the state banking system; ensuring safety and soundness; promoting economic growth and consumer protection; and fostering innovative state regulation of the financial services industry.

State regulators charter and supervise 79 percent of all banks in the United States. In addition, state regulators license and supervise a variety of non-depository financial services. CSBS, on behalf of state regulators, also operates the Nationwide Multistate Licensing System (NMLS) to license and register those engaged in mortgage, money transmission, consumer finance, debt collection, and other non-depository financial services industries. Currently, 64 state agencies use NMLS to manage 461 different license authorities covering a broad swath of nonbank financial services. NMLS is a key part of Vision 2020, our members' commitment to bringing modernized and harmonized non-bank licensing and supervision by leveraging technology and smart regulatory policy to transform the interaction between industry, regulators and consumers.

As discussed in this letter, for many years, states have been at the forefront in advancing data privacy and security for the protection of consumers residing in their states. Accordingly, we believe any federal proposal relating to the collection, use and protection of consumer data must preserve the role for state leadership in the areas of data privacy, security and control.

Federal Law Appropriately Establishes a Federal Floor in the Areas of Data Privacy, Security and Control

Data privacy and security is a dynamic field with novel risks emerging on a constant basis. It is critical that state regulators and state law enforcement agencies retain the ability to protect consumers in their states.

In enacting federal privacy laws, Congress has traditionally recognized the important role filled by the states in setting data breach standards. For example, Title V of the Gramm-Leach-Bliley Act (GLB) requires financial institutions to implement a risk-based response program to address instances of unauthorized access to consumer information systems.[1] Importantly, Section 507 of GLB establishes a floor for data breach and data security laws and expressly reserves the right of states to enact more stringent data breach and privacy laws for the protection of their citizens.[2]

Section 507 was enacted to ensure states retain flexibility to develop regulatory approaches to protecting consumer information that fairly balance the needs of business with the level of privacy protection desired by the consumers residing in their state. Accordingly, federal consumer privacy standards have operated concurrently with more stringent state data breach and privacy laws for close to two decades. The rapid evolution and proliferation of online financial services since the enactment of GLB has made it more crucial states be permitted to serve their constitutional role as "laboratories of democracy" in calibrating the appropriate level of protection for consumer data over and above baseline national standards.

In enacting federal credit reporting laws, Congress has likewise recognized the important role served by states in advancing the rights of consumers with respect to the collection, use and dissemination of consumer information by credit reporting agencies. As with federal privacy laws, the Fair Credit Reporting Act (FCRA)[3] likewise establishes a federal floor which allows for state laws to impose more stringent requirements with respect to the collecting, distribution, or use of any information on consumers or for the prevention or mitigation of identity theft.[4]

Although, over two decades ago, legislation was introduced to preempt all state laws regulating credit reporting agencies, fortunately, this initiative failed.[5] Had the initiative succeeded, critical state reforms related to credit reporting would never have been established: consumers would not have nationwide free credit reports, consumers would not have access to their credit score, consumers would have not had data breach notices, and, at least until 2018, consumers would not have the free nationwide credit freezes.

The critical lesson here is that, while Congress often waits to enact critical consumer protections until widespread consumer harm is realized, a federal floor embraces the inherent nimbleness of state law by allowing states to experiment with innovative approaches to advancing the ability of consumers to control the use of their information as novel threats emerge. For this reason, CSBS would strongly oppose any federal proposal which seeks to preempt states from playing a leading role in advancing consumers protections in the areas of data privacy, security, and control.

---

[1] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, tit. V, 113 Stat. 1338, 1436-1450 (1999) (codified as amended at 15 U.S.C. §§ 6801-6827).
[2] *See* 15 U.S.C. § 6807.
[3] *See* Fair Credit Reporting Act of 1970, Pub. L. 91–508, title VI, Oct. 26, 1970, 84 Stat. 1127-1136 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).
[4] *See* 15 U.S.C. § 1681t.
[5] *See* Consumer Credit Reporting Act of 1991, H.R. 3596, 102nd Cong., § 118 (1992).

Recent State Actions Demonstrates State Leadership in the Areas of Data Privacy, Security and Control

Recent actions by state legislators and state regulators bear out the critical role served by the states in the areas of data security, privacy and control. Each of the initiatives highlighted below are examples of states responding to emerging threats to data privacy, security and control in areas where Congress and federal regulators have failed to or lack the authority to act.

In 2016, the New York Department of Financial Services (NYDFS) proposed a comprehensive cybersecurity regulation for financial institutions.[6] This regulation—the first of its kind in the nation—is designed to protect the cybersecurity of banks, insurance companies, and other financial institutions regulated by NYDFS. The regulation requires regulated companies to establish cybersecurity programs and policies, conduct annual cybersecurity assessments, and take other specific steps to secure information and network. By taking a risk-based approach focused on highly sensitive information, the NYDFS regulation provides an incentive for companies to more effectively allocate their cybersecurity resources. The NYDFS cybersecurity regulation is just one example where the states are taking decisive action to protect consumers and our financial system in an area of data security where the federal government has yet to act.

In 2018, California enacted the California Consumer Privacy Act (CCPA) to enhance consumers' rights to control the use, including the sale, of their personal information.[7] The CCPA (which like the NYDFS cybersecurity regulation is the first law of its kind in the nation) requires companies with California residents as customers to abide by heightened disclosure standards and gives consumers considerable control over how their personal data is used.[8] The CCPA is another example of states taking the lead to develop robust, innovative solutions to ensure consumers retain control over the use and dissemination of their information.

There is an abundance of other recent examples of states taking a leadership role by enacting state laws that enhance consumer protections in the areas of data privacy, security and control. In 2018, Colorado enacted data security standards requiring companies to maintain reasonable security practices and appropriately dispose of documents containing consumers' personal information and ensure data is protected when transferred to third parties.[9] Vermont enacted a law regulating data brokers in 2018 which requires data brokers which buy and sell consumer information to register with the state's attorney general, to make annual disclosures regarding privacy practices and data breaches, and to maintain a comprehensive information security program.[10] Finally, in 2017, New Jersey enacted a law that limits a

---

[6] *See* Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500 (2017), available here: https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[7] *See* California Consumer Privacy Act of 2018, SB 1121 (2018), available here: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[8] The CCPA provides consumers with control over their information in four ways: (1) business must provide notice to consumers concerning the collection, use and dissemination of personal information; (2) consumers must be presented with a process to opt-out of having their personal information sold to a third party; (3) consumers may request that a business (or a third-party contractor) delete their personal information and must be informed of this right; and (4) businesses cannot discriminate against consumers for their exercise of rights under the CCPA.

[9] *See* Protections for Consumer Data Privacy, HB18-1128 (2018), available here: https://leg.colorado.gov/bills/hb18-1128.

[10] *See* An Act Relating to Data Brokers and Consumer Protection, H.764 (2018), available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/06/H-0764.pdf.

merchant's ability to collect information about shoppers and pass that data onto third parties.[11] These are important initiatives that demonstrate the critical role of preserving the role of states in experimenting with expanded consumer protections in the areas of data privacy, security, and control.

In addition to the above-mentioned state laws, state regulators have also been active in responding to incidents that reveal weaknesses in data security practices by existing companies. For instance, in 2018, after the large-scale data breach at Equifax was made public, eight state financial regulators entered into a consent order with Equifax to address serious deficiencies in the company's cybersecurity program that results in the breach.[12] The consent order arose from a joint examination these regulators performed of the company. The order, which applied to Equifax's operations nationwide, directed Equifax to undertake a restructuring of its risk management processes, strengthen internal controls, and enhanced Board oversight of its information security program. Thus, as with state law, the corrective actions required of Equifax demonstrates just how critical it is to preserve the ability of state regulators to take swift action when material weaknesses and emerging threats come to light.

Federal Law Must Continue to Establish a Federal Floor, Not a Ceiling, in the Areas of Data Privacy, Security and Control

For the reasons discussed above, state regulators believe it is incredibly important for federal law to continue to establish a floor for consumer protection in the areas of data privacy, security and control and, thereby, leave room for states to establish more stringent consumer protections and to act quickly as novel threats emerge. Conversely, we would strongly oppose any federal proposal that would preempt the state's authority to enact more stringent standards and enforce those standards.

State regulators stand ready to work with Congress concerning where uniformity in the areas of data privacy, security and control can be achieved while preserving the ability of states to take a leadership role in standard-setting, oversight and enforcement. Relatedly, given the experience of state regulators discussed above, any federal proposal which directs federal agencies to promulgate federal standards in the areas of data security, privacy and control should provide for a role for state regulators in the development and promulgation of those standards. Finally, if greater uniformity in data privacy, security and control is a goal, Congress should consider adopting an amendment to the Bank Service Company Act (BSCA) which would enable the sharing of examination reports and supervisory information between state and federal regulators of bank service companies and third-party service providers. Bi-partisan legislation amending the BSCA to encourage information sharing between state and federal regulators passed the House Financial Services Committee in the previous Congress by a unanimous vote of 56-0.[13]

Conclusion

CSBS appreciates the opportunity to comment in response to your request for feedback on the collection, use and protection of sensitive information by financial regulators and private companies. As discussed above, data security, privacy and control are an evolving area in which threats emerge and change with

---

[11] *See* Personal Information and Privacy Protection Act, S913 (2017), available here: https://www.njleg.state.nj.us/2016/Bills/S2000/1913_R2.PDF.

[12] For more information on Equifax Consent Order, please visit https://www.csbs.org/state-regulators-enter-consent-order-equifax.

[13] CSBS's suggested amendment to the BSCA has been proposed in The Bank Service Company Examination Coordination Act of 2017, H.R. 3626, 115th Cong. (2018), available here: https://www.congress.gov/bill/115th-congress/house-bill/3626.

great frequency, and states—due to their greater flexibility and nimbleness—have been very active in leading efforts to enhance consumer protections in this area and responding to threats to consumer protections as they emerge. Accordingly, as your offices consider what, if any, federal solutions may be appropriate in this area, CSBS urges you to bear in mind that any long-term, viable solution should preserve the ability of states to act, as they have so often, as leaders and first-responders in the areas of data security, privacy and control.

Sincerely,

John Ryan
President and CEO

1129 20th Street, N.W. • Ninth Floor • Washington, DC • 20036
www.csbs.org • 202-296-2840 • FAX 202-296-1928