May 1, 2019

The Honorable Roger Wicker
Chairman
Committee on Commerce, Science, & Transportation
512 Dirksen Senate Office Building
U.S. Senate
Washington, D.C. 20510

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, & Transportation
512 Dirksen Senate Office Building
U.S. Senate
Washington, D.C. 20510

Dear Chairman Wicker and Ranking Member Cantwell:

On behalf of the Consumer Bankers Association (CBA), I write to share our views on a national data privacy framework for the Senate Commerce, Science & Transportation Committee's hearing entitled "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework." CBA is the voice of the retail banking industry whose products and services provide access to credit for consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans, and collectively hold two-thirds of the country's total depository assets.

The State of Data Privacy

In light of recent data breaches and abuses, consumers are rightly concerned about the manner in which their personal information is being collected and how this sensitive information is being both shared and protected. In 2018 alone, the number of data breaches in the U.S. totaled more than 1,200 according to the Identity Theft Resource Center. No industry was immune from breaches in 2018: business sector (46 percent), healthcare/medical industry (29 percent), banking/credit/financial industry (11 percent), government/military (8 percent), and the education sector (6 percent). However, it is important to note that the non-financial business sector, which is not subject to national data security requirements, was responsible for the overwhelming majority (93 percent) of the personal records compromised. In addition to breaches, there have been several noteworthy examples of misuse of customer data in the past year which warrant a review of industry practices and the scope of federal privacy laws and regulations, e.g. Cambridge Analytica gained access to private information on more than 50 million Facebook users.[1]

CBA members take seriously their responsibility to clearly explain the uses of consumers' data and to safeguard it against improper use and criminals attempting to steal it. Since the passage of the Gramm-Leach-Bliley Act (GLBA) in 1999, financial institutions have been required to provide their customers a clear privacy notice detailing information collection and sharing practices, which includes an opt-out for the sharing of information with non-affiliated third parties. This notice is provided at the beginning of the customer relationship and annually thereafter. GLBA and subsequent regulations also require banks to have in place data security protocols to safeguard sensitive consumer information and to report to federal authorities and affected consumers when a breach occurs. Banks are examined by their prudential regulators on these standards and if found to be non-compliant may face fines or other penalties.

The low breach-rate of personally identifiable information (PII) at financial institutions compared to other sectors can be attributed to the common-sense safeguards required by GLBA and the industry's commitment to security. As a

[1] https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

result, consumers trust financial institutions more than any other type of organization to keep their financial information secure, according to an August 2017 poll by Morning Consult.

Consumer Privacy

CBA supports consumers having reasonable control concerning the collection, use and sharing of personal data. However, we caution against national privacy legislation that may inhibit banks' ability to fulfill their contractual obligations to consumers. Compared to other industries, banks are subject to more stringent rules and lead in protecting consumers' PII and their privacy.

Pursuant to the GLBA, banks are required to protect the security and confidentiality of consumer records and information, and the law also requires banks to disclose their privacy practices and limits sharing PII with nonaffiliated third parties. Any Federal privacy law must consider the GLBA and other existing Federal privacy laws and preempt the growing patchwork of state laws that provide differing and inconsistent consumer protections. Otherwise, a consumer's privacy protections, including their ability to understand their rights, will depend on the state where the individual resides. While these state laws may be well-intentioned, they must be crafted to not hinder the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

As Congress considers the creation of a national data privacy framework, we must first recognize the differences in data collection among industries. Banks are required by federal law to collect certain information to conduct a customer transaction. For example, if a consumer wants to open a checking account, at a minimum pursuant to the Bank Secrecy Act, the bank must obtain certain information to fulfill its Customer Identification Program requirements, such as date of birth, address, and identification number. As an additional benefit to customers, banks also use personal data to develop banking products and services that are customized to a customer's needs. Utilizing consumer data to conduct financial transactions authorized by the consumer is far different than a social media platform collecting consumer data to sell to marketers.

It is also important that a federal privacy standard should not expand the scope of data that banks are responsible for protecting. GLBA requires banks to protect consumers "nonpublic personal information", which is defined, in part, as "[. . .] personally identifiable financial information, (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[2] Consumer is defined to mean "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personally, family, or household purposes, or that individual's legal representative."[3] An expansion of the definition of covered data or covered persons pursuant to a national standard would subject banks to unnecessary regulatory burden.

A national data protection and privacy law must also seek to promote innovation, investment and competition in the marketplace. The United States Constitution authorizes Congress to regulate interstate commerce, which includes the free flow of goods, services and consumer data. A patchwork of privacy laws at the state level will lead to higher costs for consumers and create barriers to innovation and investment. The assumption that preemption weakens existing state laws is a fallacy. In a world that is increasingly mobile, Americans and their devices constantly cross state borders. Consumer protection should not depend upon which state you reside, but consumers should be covered by one unified, comprehensive federal standard.

---

[2] https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=15-USC-697127498-1137964384&term_occur=2&term_src=title:15:chapter:94:subchapter:I:section:6801

[3] https://www.law.cornell.edu/uscode/text/15/6809#4_A

From an international perspective, CBA also supports an open global economy that enables growth through the secure and efficient transfer of data across international borders. National data protection and privacy legislation should continue to support consumer privacy while also respecting and coordinating differences between U.S. and foreign privacy regimes.

National data protection and privacy legislation should be enforced by the Federal Trade Commission (FTC), unless a determination is made that it is appropriate for a different regulator to be the enforcement agency, e.g. prudential regulators for banks and credit unions. CBA is concerned that if state attorneys general are allowed to bring enforcement actions in federal court, there is a risk that each state will enforce the law differently. In addition, a national consumer privacy law should not provide for a private right of action.

Lastly, the California Consumer Privacy Act is the first major consumer privacy law to be adopted at the state level. This legislation was written hastily, and the state government is currently reviewing and revising portions of the law through both legislative and regulatory processes. As the California privacy law continues to evolve, it would be prudent for Congress to monitor issues with implementation and use their observations to draft a federal data privacy and security standard. Considering the importance of this issue and the impact it will have on both consumers and businesses, it is imperative that Congress is thoughtful in drafting meaningful legislation to protect consumers and provide businesses with certainty.

Data Security and Breach Notification

It is also critical that any conversation around data privacy also take seriously the security of data and the protocol for notifying customers in the event of a breach. Banks are on the front lines consistently monitoring for fraud and working to make consumers whole, no matter where a breach occurs. From operating advanced fraud monitoring systems to reissuing cards, CBA members spend considerable resources on preventing fraud. As a result, consumers rely on their financial institutions to communicate what to do in the event of a breach and to employ defenses to prevent fraud and identity theft.

Subsequent to Section 501(b) of GLBA, the financial regulators issued guidelines requiring banks to implement comprehensive, risk-based information security programs that include administrative, technical and physical safeguards to protect customer information. These safeguards are not static but flexible and scalable – applying to banks of all sizes. A similar framework should be applied to non-bank companies to ensure consumers' sensitive information is protected throughout the payment system.

Banks must also implement a risk-based response program in the event of a breach. The program includes an evaluation of the incident and an effort to prevent further unauthorized access as well as notice to the institution's primary federal regulator, appropriate law enforcement, and, importantly, the customers whose information was breached and could be misused. CBA supports legislation to require others in the payment system to provide timely notification to their customers in the event of a breach.

Today, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of a security breach of information involving PII.[4] Twenty-four states currently have data security laws requiring a level of security procedures and practices to be in place to protect personal information.[5]

[4] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[5] http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

Congress has the constitutional authority to regulate interstate commerce through the Commerce Clause, which was written to prevent fragmentation of markets and to encourage the free flow of goods and services, including information, across the nation with minimal interference. Congress should take seriously its authority and enact a federal data security and breach notification standard and preempt the current patchwork of state laws. With the recent breaches that have put millions of consumers at risk, the need to pass legislation to establish such a standard could not be more evident. Protecting consumer information is a shared responsibility of all parties involved.

On behalf of our members, I would like to thank you for your consideration of our views. We look forward to working with the Committee to foster an environment that prioritizes the protection and privacy of consumer data while promoting consumer access to credit.

Sincerely,

Richard Hunt
President and CEO
Consumer Bankers Association