March 15, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
U.S. Senate
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
U.S. Senate
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the Consumer Bankers Association (CBA), I write to share feedback on your request for information on data privacy, protection and collection. 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. While this total decreased from over 1,600 in 2017, the number of records exposed by these breaches more than doubled – from 198 million to 447 million records. The most common form of data breach was due to criminals hacking into systems using phishing or malware. 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 was responsible for 93% of the 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.

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 and credit unions 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 and credit unions 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 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.

Data Security and Breach Notification

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 and credit unions to implement comprehensive, risk-based information security programs that include administrative, technical and physical safeguards to protect customer information. Examples of these safeguards include, but are not limited to, the following: access controls on customer information systems; access restrictions at physical locations containing customer information; encryption of electronic customer information; dual control procedures; segregation of duties and background checks; monitoring procedures to detect actual and attempted attacks; response programs that specify certain actions; and measures to protect against destruction, loss, or damage of customer information. These safeguards are not static but flexible and scalable – applying to banks and credit unions of all sizes.

Banks and credit unions 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.

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.[1] Each of these security breach laws contains provisions regarding who must comply; a definition of PII; what constitutes a breach; notice requirements; and any exemptions. Twenty-four states currently have data security laws requiring a level of security procedures and practices to be in place to protect personal information.[2]

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 standard to protect consumer data across the payment system and preempt the current patchwork of state laws. With the recent data security 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.

CBA supports data security and breach notification legislation encompassing the following elements:

- A flexible, scalable standard for data protection that factors in (1) the size and complexity of an organization, (2) the cost of available tools to secure data, and (3) the sensitivity of the personal information an organization holds.
- A notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators when there is a reasonable risk that a breach of unencrypted personal information exposes consumers to identity theft or other financial harm.
- Consistent, exclusive enforcement of the new national standard by the Federal Trade Commission (FTC), other than for entities subject to state insurance regulation or who comply with GLBA or the Health Insurance

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

Portability and Accountability Act of 1996/HITECH Act. For entities under its jurisdiction, the FTC should have the authority to impose penalties for violations of the new law.

- Clear preemption of the existing patchwork of often conflicting and contradictory state laws.

CBA urges Congress to move swiftly to enact legislation to create a uniform national standard to ensure consumers' sensitive information is protected throughout the payment system.

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 hinder the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

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."[3] An expansion of the definition of covered data 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.

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 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,

[3] 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

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.

Consumer Credit Reporting

There has been increased regulatory and legislative attention to the business of credit reporting in light of recent breaches. The FTC and the Consumer Financial Protection Bureau are currently pursuing penalties for a recent large scale breach of consumer credit report information. On the legislative front, the Senate Banking Committee took an active role in granting consumers greater control over their credit reports with the passage and enactment of the Economic Growth, Regulatory Relief, and Consumer Protection Act (S. 2155). In the 116th Congress, additional legislation has been introduced which greatly expands the ability of consumers to remove adverse credit events from their credit reports.

It is important that a consumer's credit report be an up-to-date, accurate, and complete credit history for lenders to determine a consumer's ability to repay a loan. Lenders consider many factors when determining credit risk and may weigh credit data differently depending on their individual underwriting models. However, lenders are unable to use their discretion to properly identify and manage risk when the use of certain data is restricted. For instance, legislation seeking to reduce the amount of time adverse information can stay on reports and to clear certain adverse information harms lenders' ability to make informed credit decisions. Lenders constantly update credit models to paint the most complete picture of a consumer's creditworthiness, and overly-restrictive limits on the data lenders may use to make credit decisions will harm both lenders and consumers throughout the credit process.

Additionally, there could be safety and soundness implications of legislative efforts to remove adverse information as lenders make loans with less information, leading to loans that may be at greater risk for default. Lending involves risk; sound underwriting practices insulate financial institutions from excessive risks that lead to increased credit losses. Reduced credit losses lead to safer and better-priced products for those consumers who can truly manage them.

While CBA respects the aim of increasing consumers' control of their financial information, we caution against legislation that adds significant new compliance burdens by creating obligations of furnishers to retain specific records on consumers, mandating new and potentially frequent disclosures on the furnishing of adverse information, and expanding dispute resolution processes. Additionally, legislative proposals to permit frivolous complaints and litigation to tie up the dispute resolution process are cause for concern. Such provisions will ultimately lead to worse credit modeling, which in turn will result in less reliable decisions on consumers' creditworthiness, putting their financial well-being at risk.

On behalf of our members, I would like to thank you for your consideration of our views. We look forward to working with you 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