December 4, 2019

Statement for the Record

On Behalf of the

American Bankers Association

before the

Commerce, Science, and Transportation Committee

of the

United States Senate

Statement for the Record

On behalf of the

American Bankers Association

before the

Commerce, Science, and Transportation Committee

of the

United States Senate

December 4, 2019

Chairman Wicker, Ranking Member Cantwell, and members of the Committee, the American Bankers Association ("ABA") appreciates the opportunity to provide its views on federal privacy legislation for your December 4, 2019 hearing "Examining Legislative Proposals to Protect Consumer Data Privacy". The American Bankers Association is the voice of the nation's $18 trillion banking industry, which is composed of small, regional and large banks. Together, America's banks employ more than 2 million men and women, safeguard $14 trillion in deposits and extend more than $10 trillion in loans.

Our members are strong proponents of protecting consumer data and privacy, and financial institutions have been subject to extensive federal privacy and data protection laws and regulations for several decades. Congress carefully constructed this regulatory regime to provide an effective and successful balance between strong consumer protections while ensuring that consumer financial transactions take place in a safe and secure environment. We commend you for your interest in legislation that would put in place similar consumer protections for all entities that collect and use sensitive consumer information, and recommend that the following key elements be included in any legislation passed by Congress.

Elements of Privacy Legislation

The U.S. financial sector is subject to a number of federal laws that already impose privacy and data security obligations with respect to financial data and other data relating to consumers, particularly Title V of the Gramm-Leach-Bliley Act (GLBA). Notably, the GLBA requires that financial institutions provide consumers with notice of their privacy practices and generally prohibits such institutions from disclosing financial and other consumer information to third parties without first providing consumers with an opportunity to opt-out of such sharing. The GLBA contains strict security and confidentiality requirements over consumer records and requires notice to consumers if a breach of sensitive financial information puts them at risk. Even more significant, bank regulatory agencies routinely conduct examinations regarding compliance with the GLBA and other privacy laws, ensuring compliance in a manner that is not replicated in other sectors.

As discussed below in detail, ABA supports legislation to protect consumer privacy that includes the following elements:

- **Privacy Rights.** A national privacy standard that recognizes the strong privacy and data security standards that are already in place for financial institutions under the GLBA and other federal financial privacy laws and avoids provisions that duplicate or are inconsistent with those laws. A national standard will help consumers understand their rights.

- **Provide Strong Data Protection and Breach Notice.** Ensure that all entities that handle sensitive personal information are required to protect that data and provide notice in the event of a breach that puts consumers at risk.

- **Robust Enforcement.** Provide robust, exclusive enforcement of this national standard by the appropriate federal regulators, including preserving the GLBA's existing administrative enforcement structure for banks and other financial institutions.

- **Clear Preemption.** Preempt state privacy and data security laws to ensure that a national standard provides consistent protection for all Americans, no matter where they reside.

I. Privacy Rights

In enacting the GLBA in 1999, Congress stressed that privacy and data security is critical within the financial industry. *See* 15 U.S.C. § 6801(a) (stating that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information").[1]

It was the intent of Congress that a financial institution's privacy practices must be readily accessible and easy to understand ("transparent") so that consumers could make well-informed choices. To this end, the GLBA requires financial institutions to provide clear and conspicuous notice to their customers about, for example, their information collection and sharing practices along with the customer's rights, where applicable, to limit sharing with nonaffiliated third parties and affiliates and to limit affiliate marketing.

In addition to providing GLBA privacy notices where required (e.g., providing annual notices to customers), most financial institutions also make their GLBA privacy notices easily accessible on their websites. In terms of the form and content of notice, many financial institutions provide the disclosures using a standardized model template issued by the Consumer Financial Protection Bureau (the "Bureau") which was developed after extensive consultation with all affected stakeholders, including consumers. The Bureau's model template is designed to follow the same easy-to-understand format used for nutrition labeling on food products, and was originally developed after study and testing by the federal banking agencies. We believe that similar transparency around data collection, information sharing and information security that is

[1] *See,* http://uscode.house.gov/view.xhtml?req=(title:15%20section:6801%20edition:prelim)

provided under the GLBA should be available to consumers regardless the type of company with which they interact or do business. For purposes of federal privacy legislation, the GLBA should be considered a tried-and-true model for transparency.

The GLBA also includes carefully crafted exceptions from its limitations on sharing information with nonaffiliated third parties. The exceptions adopted by Congress are designed to ensure that financial markets function properly and that financial institutions are able to provide consumers with the products and services that they expect. Access to these products and services depend on the flow of appropriate financial information and ultimately benefit the consumer, financial markets and the U.S. economy generally. For example, the GLBA permits the disclosure of customer information to a nonaffiliated third party "as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes," in connection with "[s]ervicing or processing a financial product or service that a consumer requests or authorizes" (*e.g.*, sending a payment card transaction authorization to a merchant) or "[m]aintaining or servicing the consumer's account with" the bank (*e.g.*, working with a vendor to mail monthly statements). For example, in order to process a credit card transaction, certain key financial information must be exchanged to allow the appropriate account to be debited and the appropriate merchant credit for the transaction.

The exceptions are also designed to ensure compliance with other legal and regulatory mandates and the sharing of information to prevent fraud and illicit finance, while not hindering lawful commerce. For example, the exceptions are designed to allow financial institutions to share information with state authorities seeking to enforce child support payments and to share important information with the Financial Crimes Enforcement Network (FinCEN) about suspicious activities as a means to combat money laundering and other illicit finance. Notwithstanding these exceptions, to protect consumers, the GLBA generally prohibits the disclosure of a customer's account number or access code for a consumer's credit card account, deposit account, share account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through e-mail.

However, GLBA is not the only federal privacy statute that applies to the financial sector. The financial sector has long been subject to other federal financial privacy and data protection laws, including the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA), both of which were enacted initially in the 1970s. The FCRA, among other things, restricts the collection, use, and sharing of information that is used to determine a consumer's eligibility for, among other things, credit, insurance, and employment. The FCRA functionally limits the extent to which affiliated financial institutions may share with each other information relating to their customers, and requires financial institutions to give customers notice and the opportunity to opt-out of the sharing of certain information (*e.g.*, application and credit report information) among affiliates and to opt-out of the use of such information for marketing purposes.

Separately, the RFPA protects individuals against unwarranted searches of personal financial records by the federal government. For example, a bank may not provide a federal government entity with access to copies of, or the information contained in a customer's financial records except as permitted by the RFPA (*e.g.*, in response to a search warrant). In addition, while RFPA is limited to federal access to financial records, most states have similar laws that extend these protections by limiting the disclosure of financial records to state government entities.

There are still other federal laws that may come into play. Depending on their specific activities, a financial institution also may be subject to a host of other federal privacy laws, including the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the CAN-SPAM Act, the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, and the Driver's Privacy Protection Act, among others.

Therefore, it is clear that Congress has long recognized the importance of privacy for financial institutions and has put in place several meaningful frameworks that include strong privacy protections balanced with commonsense exceptions to minimize marketplace disruptions, as well as strong data security protections. While ABA supports legislation to put in place a national privacy standard, that standard must recognize the strong privacy and data

security standards that are already in place for the financial sector under the GLBA and other financial privacy laws and avoid provisions that duplicate or are inconsistent with those laws. We likewise believe that any such national standard should include the GLBA's established exceptions that ensure the efficient operation of our local and national financial markets that serve consumers and businesses so well. Any departure from the existing framework will be disruptive to the economy.

II. Provide Strong Data Protection and Consumer Notice

Over the past few years, major breaches of personal information at a wide range of nonbank entities, including government agencies, have put literally hundreds of millions of consumers at risk.[2] The financial sector believes strongly in protecting consumers' sensitive personal and financial information. For hundreds of years, customers have relied on financial institutions to protect their financial information. Because banks are literally at the center of people's financial lives, our industry has long been subject to federal data protection laws and oversight. For example, along with the privacy protections mentioned above, the GLBA also requires the federal regulatory agencies to establish standards for safeguarding customer information. These standards require financial institutions to ensure the security and confidentiality of customer information, protect against any anticipated threats to such information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Moreover, since April 1, 2005, the federal banking agencies have required banks to have in place incident response programs to

[2] For example, in 2018 alone major data breaches took place at social media platforms, retailers, airlines, health care companies, government vendors and other online businesses. Some of these include Facebook, Google, Quora, MyFitnessPal, Marriott, Cathy Pacific (airline), Delta, Saks Fifth Avenue, Chegg (online textbooks), GovPayNow and United Point Health. Source: Identity Theft Resource Center https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/

address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Looking toward the future, there is no doubt that technology is fundamentally changing how financial services are delivered. Customers are adopting new technologies and are relying increasingly on these new technologies to interact with their financial institutions. Mobile access and digitization of traditional services have brought an explosion in the amount of financial data being created. It is important, however, to ensure that bank-like protections are built into these applications. ABA members are engaged in partnering with fintech companies and as a result, consumers have benefitted from innovative products and services.

For ABA members, regardless of the commercial or government entity involved, it is vital that privacy legislation requires all entities handling sensitive personal information implement and maintain adequate security measures to protect that information and provide notice to individuals who are subjected to harm resulting from a breach of their information.

III. Robust Enforcement

Compliance by banks with GLBA and other privacy laws is regularly examined by the bank regulatory agencies. Unlike other sectors, where violations of statutory and regulatory restrictions must occur before attention is given to compliance, banks are subject to strict regulatory oversight and regular exams regarding their compliance with privacy and data protection laws.

The federal banking agencies have formal procedures that govern bank examinations. For example, this oversight includes the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook, which is an extensive document with over 1,000 pages of IT guidance and examination instructions used by bank regulators to determine bank compliance with, among other things, vendor management, IT governance and information security program management.[3]

[3] https://ithandbook.ffiec.gov/

If a bank fails to comply with the GLBA, the federal banking agencies can bring enforcement actions to recover significant penalties. Specifically, compliance with Section 501(b) of the GLBA is enforced by the federal banking agencies under Section 8 of the Federal Deposit Insurance Act ("FDIA").[4] The federal banking agencies can bring an enforcement action alleging that a failure to comply with the Guidance is an unsafe or unsound practice. In this regard, Section 8 of the FDIA[5] includes various penalties and remedies for an unsafe or unsound practice, including:

(1) a cease-and-desist order;

(2) an order requiring that the financial institution correct or remedy any conditions resulting from the unsafe or unsound practice;

(3) Removal or suspension of bank parties from office;

(4) a civil penalty of $5,000 for each day in which the financial institution violates a cease-and-desist order or order requiring the correction of an unsafe or unsound practice;

(5) a civil penalty of $25,000 for each day in which the financial institution recklessly engages in an unsafe or unsound practice; and

(6) up to $1,000,000 or 1 percent of assets for knowingly engaging in an unsafe or unsound practice.

[4] 15 U.S.C. § 6805(a).
[5] 12 U.S.C. § 1818.

Therefore, ABA members do not support recommendations that would give privacy enforcement authority over banks to other federal agencies, such as the Federal Trade Commission (FTC), or state Attorneys General or other state and local government authorities.

It is important that any privacy legislation containing a national standard must provide robust, exclusive enforcement of this national standard by the appropriate federal or state regulators across all industry sectors. This must include preserving GLBA's existing administrative enforcement structure for financial institutions, including banks.

IV. Clear Preemption

The increasing patchwork of state privacy and data breach laws must be replaced by a federal standard. In our view, it is critical that any new federal privacy law preempt existing state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system. A federal standard will also help increase the transparency needed for consumers to understand their rights and responsibilities. Equally important, having a federal standard would ensure that consumers receive the same privacy rights and data protections regardless of where they may live. Allowing each state to enforce federal consumer privacy rights guarantees that within a short period, different standards will apply in the various states due to court interpretation of statutory law. As a result, the protections for someone in Virginia may differ from those across the river in Maryland.

CONCLUSION

ABA supports legislation to protect consumer privacy that would put in place a national privacy standard that recognizes that strong privacy and data security standards are already in place for financial institutions under the GLBA and other financial privacy laws and avoids provisions that duplicate or are inconsistent with those laws. The national privacy standard must ensure that all entities that handle sensitive personal information are required to protect that data and provide notice in the event of a breach that puts consumers at risk. It must also provide robust, exclusive enforcement of this national standard by the appropriate federal or state

regulators, including preserving GLBA's existing administrative enforcement structure for financial institutions, including banks. Finally, the national privacy standard must eliminate the current inconsistent patchwork of state laws on privacy and data security. A national standard containing these elements would provide consistent protections for consumers and will enhance their understanding of their privacy rights.