Statement for the Record

On behalf of the

American Bankers Association

before the

Committee on Commerce, Science, and Transportation

United States Senate

February 27, 2019

American Bankers Association

Statement for the Record

of the

American Bankers Association

for the

Committee on Commerce, Science, and Transportation

United States Senate

February 27, 2019

Chairman Wicker, Ranking Member Cantwell, and members of the Committee, the American Bankers Association ("ABA") appreciates the opportunity to provide its views on consumer data protection and privacy. The ABA is the voice of the nation's $17 trillion banking industry, which is comprised of small, midsized, regional and large banks. Together, these institutions employ more than 2 million people, safeguard $13 trillion in deposits and extend more than $9.5 trillion in loans. For many years, our members have had and continue to have a substantial interest in consumer data protection and privacy and we respectfully request that this statement be included as a part of the record for today's hearing.

A. Banks and Financial Institutions Are and Have Been Subject to Extensive Privacy Laws

Banks believe strongly in protecting consumers' sensitive personal and financial information and their privacy. For hundreds of years, customers have relied on banks to protect the privacy of their financial information. Because banks are literally at the center of people's financial lives, our industry has long been subject to federal and state data protection and privacy laws. For example, Title V of the Gramm-Leach-Bliley Act (GLBA) not only requires banks to protect the security and confidentiality of customer records and information, but it also requires banks to provide consumers with notice of their privacy practices and limits the disclosure of financial and other consumer information with nonaffiliated third parties.

In enacting the GLBA in 1999, Congress stressed how critical privacy and data security is within the financial industry.[1] In this regard, it was Congress' intent that a financial institution's privacy practices must be readily accessible and easy to understand ("transparent") so that consumers can make well-informed choices. For example, the GLBA requires banks to provide notice to their customers about their information collection policies and practices. The notice is required to be clear and conspicuous and accurately describe the consumer's right to opt-out of the sharing of personal information with non-affiliated third parties if the bank shares customer information with such parties outside of exceptions.

Most banks make their GLBA privacy notices easily accessible on their websites. In this regard, many banks provide these disclosures using a standardized model template issued by the Consumer Financial Protection Bureau that is designed to follow the same format used for nutrition labeling on food products. The current disclosures for consumers were developed over years of effort by federal regulators and the industry. Similar transparency about data collection and information sharing that is provided by the financial sector should be available to consumers no matter the type of company with whom they do business. For purposes of Federal privacy legislation, the GLBA should be considered a tried-and-true model for transparency.

In addition to transparency, the GLBA generally prohibits a bank from providing customer information to a nonaffiliated third party unless the bank has provided the customer with notice and an opportunity to opt out and the customer has not elected to opt out of such sharing. In this regard, the GLBA contains carefully crafted exceptions to the limitations on disclosures to nonaffiliated third parties that are designed to ensure that financial markets, products and services that depend on the flow of financial information function efficiently for the benefit of the consumer, the financial institution and the financial markets generally. For example, the GLBA permits a bank to disclose customer information to a nonaffiliated third party "as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes" or in connection with "[s]ervicing or processing a financial product or service that a

[1] *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").

consumer requests or authorizes" or "[m]aintaining or servicing the consumer's account with" the bank. The exceptions are also designed to ensure that banks can comply with other legal and regulatory mandates and be able to share information to prevent fraud and illicit finance. Notwithstanding these exceptions, the GLBA generally prohibits a bank from disclosing a customer's account number or similar form of access 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.

The GLBA also required 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. And, since April 1, 2005, the federal banking agencies have required banks to have in place incident response programs to address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Banks also are subject to other, decades-old federal financial privacy and data protection laws, including the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA). 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 or employment. The FCRA functions to limit the extent to which affiliated financial institutions may share with each other information relating to consumers, including requiring notice and an opportunity to opt out before sharing non-transaction or non-experience information (*e.g.*, application information) that is used to determine eligibility for credit. Even to the extent that the FCRA permits affiliated financial institutions to share consumer information (*e.g.*, pursuant to notice and an opportunity to opt out), the FCRA limits the use of certain information for marketing if the information is received from an affiliate, including requiring notice and an opportunity to opt out before using the information for marketing purposes.

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). Most states have similar laws limiting the disclosure of financial records to state government entities.

In addition, depending on their specific activities, a bank 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.

Banks are also subject to strict regulatory oversight and regular exams regarding their compliance with data protection and privacy laws. This oversight includes the Federal Financial Institutions Examination Council Information Technology Examination Handbook, which is an extensive document with over 1,000 pages of IT guidance and examination instructions used by banking regulators to measure compliance with IT governance and information security program management.

In other words, the Congress has long recognized the importance of privacy for financial institutions and put into place a regulatory framework of strong privacy protections balanced with commonsense exceptions to minimize marketplace disruptions while maintaining a high level of consumer safeguards. These protections have been buttressed by a number of other laws with strong privacy protections, and banks and their federal and state regulators work aggressively to ensure consumers remain strongly protected.

We believe that it is critical that any new Federal privacy law take into consideration existing privacy laws, such as the GLBA, that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. Any new Federal privacy legislation should also preempt the existing patch work of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial

system. Equally important, having a single federal standard would ensure that consumers receive the same privacy rights and protections regardless of where they may live. A variety of state laws not only makes compliance challenging for financial institutions, but makes it very difficult for consumers to understand – and protect – their own privacy rights; the greater the variation in state laws, the greater confusion and conflict between states and the less transparent the entire regime becomes.

B. State Privacy Laws

The financial services sector is concerned that if Congress does not enact uniform national privacy standards, the states will continue to attempt to fill the void with a patchwork of disparate and inconsistent requirements. In 2018, California enacted a significant new privacy law, the California Consumer Privacy Act (CCPA), prompted by a pending ballot initiative. Although an improvement over the ballot initiative, the CCPA was enacted without adequate discussion or time to fully understand the consequences. For instance, it did not take into account the many reasons data flow is important to provide consumers with the goods and services that they need or request and lacks that careful balancing that it needed. It is that balancing that is inherent in the exceptions that Congress created in GLBA.

It is important to note that the California legislature included a GLBA exception in recognition of the fact that banks and other financial institutions are already subject to Federal privacy laws and already take important steps to protect consumers' privacy rights. However, concerns remain. For example, the reach of the new law is very broad and will be subject to interpretation in implementing regulations and litigation; therefore, its full impact is uncertain. The law also includes a provision that allows consumers to request that their information be deleted, a right that could compromise law enforcement efforts to combat fraud, money laundering and terrorist financing.

Meanwhile, other states are already considering adopting privacy laws similar to, if not modeled on, the CCPA, with sufficient difference that will exacerbate the existing patch-work of different and often inconsistent state privacy and data breach laws. At this point, ten states have

introduced legislation similar to the CCPA that would provide consumers with a right to know what information is collected about them and how that information may be used. One major problem is that the definition of "consumer" and covered "personal information" is very broad and not always consistent. The CCPA defines these terms very broadly – for instance, a "consumer" can be a resident of California that is residing "for a temporary or transitory purpose" in another state. Because consumer information is not anchored within a particular state as the U.S. has a very mobile population, competing state privacy regimes are likely to provide inconsistent requirements for how that information is handled. While these laws may be well-intentioned, they hamper the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

C. International Privacy Laws

The financial services sector also supports an open global economy that enables trade, investment, and growth through the secure and efficient transfer of data across borders. However, measures that dictate where data is stored and how data is transferred can hinder the development of technology infrastructure and reduces our ability to serve our mobile customer base. Measures that "ring-fence" data or require data to remain in the country of origin, often referred to as data localization, ultimately damage the global competitiveness of the U.S. financial services sector and serve as non-tariff barriers to trade. These restrictions limit the efficiency of technology operations, as well as the effectiveness of security and compliance programs. It is unfortunate that the European Union (EU) has chosen to go down this path through its General Data Protection Regulation (GDPR), which has extra-territorial reach that potentially impacts the operations of U.S. banks both internationally and in certain cases, domestically. Furthermore, the lack of clarity makes it difficult to understand and challenging for compliance. And, like the CCPA, the GDPR includes a provision that lets consumers request that information be deleted, which, as noted, is a problem for law enforcement.

The broad and judicially untested language of GDPR may even have an impact on community banks in the U.S. For example, some community banks are starting to question how they can continue to serve academia, military, and non-English speaking communities without

running afoul of the GDPR in light of its claim to jurisdiction over people living in the EU and websites offered in an EU language. Existing U.S. customers living, working, or studying abroad, including U.S. college students enrolled at an EU university, academia, or U.S. service members and their families stationed overseas may subject a U.S. bank to GDPR restrictions. Similarly, a community bank in the Southwest offering online banking services in Spanish to a U.S.-based Mexican immigrant community, or a bank in the Northeast offering online banking services to dual U.S.-Portugal citizens that may live, work, retire or own property in both countries may be subject to the GDPR. As a result, the GDPR could potentially reduce the availability of banking services to underserved customers in the U.S.

On the other hand, increasing the global interoperability of privacy regimes can help to mitigate localization requirements while achieving regulatory policy goals. Regional agreements such as the Asia-Pacific Economic Cooperation (APEC) cross-border privacy rule (CBPR) enable commerce supported by the free flow of data, while preserving the national authority to develop privacy requirements that best serve their policy objectives. To date, the CBPR has had diminished utility since it is not global. The financial services sector could potentially support an expansion of CBPR if it includes European Union member states and other key trading partners to effectuate its potential. Similarly, consideration should be given to other well-established privacy principles currently being used by many in the financial sector to ensure interoperability, such as Privacy by Design (PbD), accountability, data retention and use limitations and protection of cross-border transfers of data.

CONCLUSION

The ABA shares the Committee's goal of protecting sensitive consumer personal and financial information and privacy. Banks and other financial institutions are already subject to the GLBA and other Federal financial privacy laws. We believe that it is critical that any new Federal privacy law take into consideration existing privacy laws, such as the GLBA, that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. Any new Federal privacy legislation should also preempt the existing patch work of state laws to

avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system and make privacy rights less transparent to consumers.