Statement for the Record

On behalf of the

American Bankers Association

Submitted for a hearing on

"Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act"

before the

Committee on Commerce, Science, and Transportation

of the

United States Senate

Statement for the Record

On behalf of the

American Bankers Association

Submitted for a hearing on

"Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act"

before the

Committee on Commerce, Science, and Transportation

of the

United States Senate

October 10, 2018

Chairman Thune, Ranking Member Nelson 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. Our members 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 Already Are Subject to Extensive Privacy Laws

Banks and other financial institutions believe very 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, the Gramm-Leach-Bliley Act (GLBA) not only requires financial institutions to protect the security and confidentiality of customer records

and information, but it also requires financial institutions to provide consumers with notice of their privacy practices and limits the disclosure of financial information with nonaffiliated third parties.

Banks also are subject to other federal privacy and data protection laws, including the Right to Financial Privacy Act, the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA). Any Federal data protection and privacy law enacted by Congress must take into account the GLBA and other existing Federal privacy laws and preempt the patch-work of state laws that provide different and often inconsistent consumer protections across the country. Otherwise, a consumer's privacy protections, including their ability to understand their own rights, will depend entirely on the state in which the individual lives.

In enacting the GLBA, 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 financial institutions to provide notice to their customers about their privacy 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. As a general practice, banks often make these notices easily accessible via websites. Many financial institutions provide these disclosures using a standardized model template designed to follow the same format used for nutrition labeling on food products. Similar transparency 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 good model for transparency

The GLBA also contains carefully crafted exceptions to the limitations on disclosures to nonaffiliated third parties that are designed to ensure that financial markets that depend on the flow of financial information function efficiently for the benefit of the consumer, the financial institution and the financial markets generally. As a result, it is critical that any new Federal privacy law take into consideration existing privacy laws that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. Any new Federal privacy legislation should recognize the GLBA and other existing Federal privacy laws and preempt the existing patch work of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system.

B. International and State Privacy Laws

The financial services sector 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.

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. For example, existing U.S. customers living, working, or studying abroad, including U.S. college students enrolled at an EU university, academics, or U.S. service members and their families stationed overseas may subject a U.S. bank to GDPR restrictions. Moreover, 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.

The financial services sector is also concerned that if Congress does not enact uniform national privacy standards, the states will fill the void with a resulting patchwork of disparate and inconsistent requirements. In 2018, California enacted a significant new privacy law, the California Consumer Privacy Act (CCPA). The CCPA was enacted very quickly and without adequate discussion or time to fully understand the consequences.

To its credit, 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. However, concerns remain. For example, the reach of the new law is very broad and will be subject to interpretation in implementing regulations; therefore, its full impact is uncertain. In addition, other states are already considering adopting privacy laws similar to, if not modeled on, the CCPA, and this will exacerbate the existing patch-work of different and often inconsistent state privacy and data breach laws. 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.

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 privacy laws. Therefore, any new Federal privacy legislation should recognize the GLBA and other existing Federal privacy laws and preempt the existing patch work of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system.