INDEPENDENT COMMUNITY BANKERS of AMERICA®

January 14, 2019

Ms. Naomi Lefkovitz
U.S. Department of Commerce
National Institute of Standards and Technology
MS 2000
100 Bureau Drive
Gaithersburg, MD 20899

Submitted electronically to
privacyframework@nist.gov

Re: NIST Docket Number 181101997-8997-01, Notice; Request for Information (RFI), "Developing a Privacy Framework"

Dear Ms. Lefkovitz:

On behalf of the Independent Community Bankers of America[1] ("ICBA"), we thank the National Institute of Standards and Technology ("NIST") for this request for information ("RFI") on "Developing a Privacy Framework". Community banks take their responsibility of protecting consumer data and privacy seriously. Banks face a multitude of regulatory requirements, along with supervision and examination, to ensure consumer data is held safely.

The RFI makes clear that the NIST Privacy Framework would be voluntary. ICBA strongly supports the voluntary nature of a privacy framework. The privacy framework will serve as a first step for companies and entities across the country that do not have a regulatory structure to require privacy standards and safeguards on their industries.

Community Banks and Privacy

By their very nature, community banks and other financial institutions must collect sensitive personally-identifiable information ("PII") about customers to meet their needs for financial services, which includes an array of deposit and loan services. This information is also used to

[1] **About ICBA**
The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. With more than 52,000 locations nationwide, community banks constitute 99 percent of all banks, employ more than 760,000 Americans and are the only physical banking presence in one in five U.S. counties. Holding more than $4.9 trillion in assets, $3.9 trillion in deposits, and $3.4 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.

prevent fraud, identity theft and comply with various regulatory requirements. Safeguarding customer information is central to maintaining public trust and retaining customers.

This letter provides a general overview of some of the legal and regulatory requirements to which banks are subject and by which they are examined and supervised. These requirements include, but are not limited to, the Gramm-Leach-Bliley Act, the "Interagency Guidelines Establishing Information Security," the Federal Financial Examination Council's IT Handbook, Electronic Funds Transfer Act, Right to Financial Privacy Act, and various state data security and privacy laws.

I. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations requires financial institutions to disclose their information-sharing practices to their customers and to safeguard sensitive data. Additionally, Section 501(b) of the GLBA requires federal banking agencies to establish standards for protecting the security and confidentiality of financial institution customers' non-public personal information.

Subtitle B of GLBA prohibits any person from receiving customer information about another person whether by making a false, fictitious or fraudulent statement to a financial institution representative, to a customer of a financial institution or providing any fraudulent document to a financial institution.[2]

II. Interagency Guidelines Establishing Information Security

The banking agencies issued "Interagency Guidelines Establishing Information Security" ("Guidelines")[3] to implement the GLBA requirements. Generally, the Guidelines establish administrative, technical and physical safeguard standards to ensure the security, confidentiality, integrity and proper disposal of customer information.

The Guidelines apply to customer information maintained by, or on behalf of, financial institutions. The Guidelines, among other requirements, mandate that financial institutions implement "a written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the bank and nature and scope of its activities".[4]

[2] 15 U.S.C. 6821
[3] 12 C.F.R. Part 30, Appendix B.
[4] Federal Register. Vol 66. No. 22. Page 8619.

The Guidelines also specify that the board of directors or an appropriate committee of the board of each insured depository institution shall be involved in approving and overseeing the written information security program.

Each institution is also required to assess risk by identifying reasonably foreseeable internal and external threats, the likelihood and potential damage of those threats and assess the sufficiency of policies, and procedures of customer information systems and other arrangements in place to control risks. There are also extensive requirements for managing and controlling the risk which include implementation of a response program.

This response program is further explained in Supplement A to Appendix B of the Guidelines. For example, banks must assess the nature and scope of an incident and notify its prudential regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information.

If a bank becomes aware, upon an investigation, that customer information was improperly accessed, it must notify the affected customers with a description of the incident and what customers may do to protect themselves.

Finally, it is also important to point out that entities contracted by financial institutions are also required to protect customer information in the same manner as the financial institution.[5]

III. Federal Financial Institutions Examination Council ("FFIEC") IT Examination Handbook, Electronic Funds Transfer Act, Right to Financial Privacy Act.

Other legal and regulatory guidance also adequately dictates bank privacy procedures. For example, the FFIEC IT Handbook is an authoritative document which outlines various guidelines concerning customer data security and privacy and they are rightly intertwined within all business operational aspects of the bank – from governance to third- party management to information technology. The Electronic Funds Transfer Act requires a disclosure to consumers when using electronic funds transfer that, in the ordinary course of doing business, the financial institution may provide information concerning the consumer's account to third parties (Section 205.7(b)(9)). The Right to Financial Privacy Act requires that a financial institution

[5] Board of Governors of the Federal Reserve System. Interagency Guidelines Establishing Information Security Standards "Small Entity Compliance Guide". 2.

provide notice to a customer before a financial institution discloses customer financial information to government authorities.

Closing

As NIST develops this privacy framework, it is essential that the existing financial services regulatory requirements, which are effective, be given the highest weight and serve as a model for other industries with no regulatory requirements in place.

Respectfully Submitted,

Jeremy J. Dalpiaz, Vice President
Cyber and Data Security Policy