February 18, 2011

Federal Trade Commission
Office of the Secretary
Room H-113
600 Pennsylvania Avenue, NW,
Washington, DC 20580

Re: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

Dear Sir or Madam:

This comment letter is submitted by the Consumer Bankers Association ("CBA")[1] in response to the Federal Trade Commission (FTC) Staff Preliminary Report on Protecting Consumer Privacy (Report), which was issued on December 1, 2010. This Report offers a framework to balance the privacy interests of consumers with innovations that rely on consumer information to develop beneficial new products and services. In addition, the Report recommends numerous other measures to improve the transparency of information practices and to help consumers who want to protect their privacy. CBA appreciates the opportunity to share its views on the Report with the FTC.

Under the current U.S. approach, the focus has been on addressing significant, sensitive, and specific privacy interests, such as fraud, personal information about children, and other inappropriate practices. Where additional concerns are identified, the FTC should not address these concerns through comprehensive new privacy laws and regulations that treat all data the same or in a similar manner. This would likely have significant repercussions for the free-flow of information, which would not only adversely affect specific business operations, but would negatively impact the economy as a whole.

To the extent a new framework is contemplated, however, the FTC should look to the cornerstone of privacy for financial institutions, the Gramm-Leach-Bliley Act (GLBA) as a model, as it strives to achieve the correct balance between providing important

[1] The Consumer Bankers Association ("CBA") is the only national financial trade group focused exclusively on retail banking and personal financial services — banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation on retail banking issues. CBA members include most of the nation's largest bank holding companies as well as regional and super-community banks that collectively hold two-thirds of the industry's total assets.

privacy protections for consumers with the understanding that certain information sharing is necessary and appropriate. As outlined below, CBA also urges the FTC to recognize the other comprehensive privacy laws and rules that currently apply to financial institutions and not seek to change this structure or add an additional layer of unnecessary regulation.

CBA also offers the following additional, specific comments in response to this Report.

A New U.S. Framework is Not Necessary

To the extent there are privacy concerns, either now or in the future, we believe the preferable approach would be to specifically address those concerns, rather than create an entirely new U.S. framework to replace the current system that we believe has worked well for consumers and businesses. Such an approach has been successful as it has continued to permit information-sharing that is appropriate and necessary for business operations, while protecting consumer privacy interests.

If it Proceeds with a new Approach, the FTC's Approach to Privacy Should Emulate the GLBA Model

The GLBA contains perhaps the most significant provisions that are appropriate and widely applicable with regard to the sharing of consumer information. These include restrictions on the ability of financial institutions to share their customer information with nonaffiliated third parties, while permitting sharing with affiliated entities. Specifically, the GLBA prohibits a financial institution from sharing a customer's personal information with a nonaffiliated third party, unless the institution has provided the customer with a privacy notice and an opportunity to opt out of the sharing. However, there are broad exceptions that recognize the legitimate need to share the information without the need to provide the opt-out right. These include, among other things, the sharing of information resulting from processing transactions and providing services, as well as to comply with legal requirements.

In addition, the GLBA includes requirements with regard to information security that are also addressed in the Report. These require each financial institution to develop and implement a risk-based information security program designed to protect the customer's information. Financial institutions must also implement programs to respond to security incidents involving customer information, including notifying customers where appropriate.

The FTC should also recognize that there is a Comprehensive Framework in Place for Financial Institutions in Addition to the GLBA Requirements

Over the years, Congress has adopted a series of laws and rules with regard to the privacy of consumer information. These significant laws and rules include the privacy protections in the GLBA, the Fair Credit Reporting Act (FCRA), the Electronic Funds Transfer Act, the Equal Credit Opportunity Act, and the Fair Credit Billing Act. For the most part, these have been careful to strike a reasonable balance between protecting

specific consumer interests with the legitimate need for financial institutions to collect and disseminate information, consistent with the operations of the institution. We see no need to change this comprehensive structure of financial privacy requirements that has been carefully crafted over the years by Congress and the financial institution regulators, and at great cost to the industry in terms of time and resources.

In addition to GLBA, the FCRA is another financial privacy law that balances the needs of the industry with the privacy concerns of consumers. The FCRA, for example, restricts the disclosure of credit report information by the consumer reporting agencies that aggregate this information, as well as the use of this information by financial institutions and others. While FCRA imposes restrictions on credit report information, it does permit the use of credit report information without consumer choice in certain situations.

The FCRA also contains provisions to ensure the information is accurate, which include requirements that consumers be provided access to the information maintained about them and the right to respond to information they believe to be inaccurate. In addition, the FCRA provides consumers with the ability to limit the sharing and use of credit report information when there may be misuse, such as when there is the potential for identity theft.

Congress just last year included additional provisions in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) that again demonstrated the intent of Congress to address the needs of consumers to have access to personal information, while recognizing the competing policy considerations. For example, the Dodd-Frank Act directs the new Consumer Financial Protection Bureau ("CFPB") to issue rules requiring a financial institution to make available to a consumer, upon request, information in the institution's control or possession concerning the financial products or services the consumer has obtained from the institution. However, there are exceptions, which include information collected by a financial institution for the purpose of preventing fraud or money laundering and any information a financial institution cannot retrieve in the ordinary course of business.

In short, there is already a very comprehensive regulatory structure and framework that applies to financial institutions. These current privacy laws and rules now serve to balance the privacy interests of consumers with the legitimate needs of financial institutions to have access to and disseminate consumer information. It makes little sense to subject the industry to new changes to these requirements, absent a compelling indication of a need.

The "Opt-Out" Approach should continue to be the Primary Method of Providing Choice with Regard to Privacy

The Report states that "staff notes that both sensitive information and sensitive users may require additional protection through enhanced consent." As also noted in the Report, "the Commission staff has supported affirmative express consent where companies collect sensitive information for online behavioral advertising and continues to believe that certain types of sensitive information warrant special protection, such as

information about children, financial and medical information, and precise geolocation data. Thus, before any of this data is collected, used or shared, staff believes that companies should seek affirmative express consent."

However, where choice is provided with respect to the use of financial information, the current regulatory structure focuses on the "opt-out" method for providing such choice. There is no reasonable basis for moving to an "opt-in" approach, as indicated by the FTC. The privacy laws and rules that have been tailored by Congress and regulators over the past several decades have been successful in protecting consumer privacy.

The Report contemplates that businesses would not need to provide choice before collecting and using consumer data for commonly accepted purposes, such as product fulfillment. We believe this should be construed very broadly as we are very concerned that consumers will be overwhelmed with choices from the various companies with which they do business, asking them whether or not they agree to multiple information uses and disclosures. We believe this would be unnecessary and confusing for consumers. Again, our preferable approach would be to provide choice only when there are specific harms that need to be addressed.

Specific Provisions in the Report with Regard to Privacy Notices

The Report indicates businesses should obtain an additional affirmative consent, or an "opt-in," before using consumer data in a materially different manner than was indicated at the time the information was collected. We believe this approach would not be in the best interests of consumers and would adversely affect business operations. Businesses have many legitimate uses of customer information that are necessary to facilitate transactions and business operations. It may be very difficult in these and other situations to identify, prior to providing notice, all of the legitimate uses of the information. However, if a business is unable to do so and fails to provide notice disclosing such uses, it may be prohibited from later using the information for a non-disclosed use, absent re-notification and consent. We do not believe this would be an appropriate approach, as there are often legitimate, reasonable, and appropriate reasons for different uses of the information, which may also be critical to the company's continued operation and generating continued economic growth, or in furtherance of certain government policy goals, such as infrastructure protection.

Although the degree of difficulty in complying with any such requirements would depend on the interpretation of "a materially different manner," we strongly prefer the current approach in which there is the presumption that customer information can be collected, used and disclosed, unless there is a specific prohibition. If there are specific uses that are viewed as harmful, they can be addressed by way of a "harms-based approach" in which these specific uses are restricted. This would be far preferable than limiting the information use to those specifically identified in a notice. In our view, any deviation from the current approach would be impractical and have a significant adverse effect on business operations.

In addition, the resulting notice under the FTC's approach would likely be much longer than current notices used by financial institutions, with information most consumers would not find relevant or helpful, the result of which would be that consumers will simply ignore or disregard them. Those who do read this information would be less likely to understand or may inadvertently bypass the information that would be helpful to them.

These issues are exactly the reasons the FTC and the other financial institution regulators recently developed model privacy notices that are intended to be simple and easy to understand by, for example, briefly indicating the possible uses of the information, such as for "everyday business purposes." This model, a project managed by the FTC, was developed over the course of five years, and included significant consumer testing. This was a huge and expensive undertaking and should not now be discarded by changing the requirements for the privacy notices that apply to financial institutions. To the extent these provisions of the Report are implemented, we strongly urge that the current privacy notices used by the financial services industry be used as the model to apply to other businesses.

This would also address another stated goal of the Report, which is the development of privacy notices that are clearer, shorter, and more standardized in order to assist consumers in comprehending and comparing privacy practices. In a related context, this is also the stated goal of Professor Elizabeth Warren, the Special Advisor to the President on the Consumer Financial Protection Bureau, with regard to agreements and disclosures for financial transactions. In a recent speech, she indicated these should be "short agreements that can be read in very little time with very high levels of understanding.[2]

Providing Consumers with Additional Access to Information May Impose Significant Costs

According to the Report, companies should provide reasonable access to the consumer data they maintain and the extent of such access should be proportionate to the sensitivity of the data and the nature of its use. Although the Report includes a "sliding scale," based on the type of information maintained and the extent to which data inaccuracies could harm consumers, we are still concerned such a requirement would require system changes in order to track this information in a manner that is searchable and can be updated, as well as additional staff training in order to respond to consumer requests. These additional costs would be much higher for those who rely heavily on paper and offline collection of data.

[2] Professor Elizabeth Warren's speech before the Financial Services Roundtable, September 29, 2010.

The Restrictions in the Report Should Not Cover Publicly Available or Business Information

The restrictions in the Report cover any data that can reasonably be linked to a specific consumer, computer, or other device. We believe this is too broad and should exclude publicly available information, as well as information a consumer may use for business purposes.

As for excluding business information from the Report, this should be acceptable since this would not adversely affect individual privacy rights. In fact, individuals acting in their professional capacity expect and would want, for example, their contact information to be shared easily with others. Imposing privacy obligations in these situations would only serve to impede the flow of business communications, which would adversely affect economic activity with little or no corresponding privacy benefits.

There is also no reason for the Report to cover information that is publicly available. Since such information is already available to the general public, it makes no sense for financial institutions to incur the costs and burdens of implementing privacy protections that would clearly provide no benefits for consumers.

Conclusion

Thank you for the opportunity to comment on the Report. If you have any questions or wish to discuss these issues further, please feel free to contact me at (703) 276-3862 or at jbloch@cbanet.org.

Sincerely,

Jeffrey P. Bloch
Senior Regulatory Counsel