

March 15, 2019

The Honorable Mike Crapo  
Chairman  
Committee on Banking, Housing  
and Urban Affairs  
U.S. Senate  
Washington, D.C. 20510

The Honorable Sherrod Brown  
Ranking Member  
Committee on Banking, Housing  
and Urban Affairs  
U.S. Senate  
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

The American Bankers Association (“ABA”) appreciates the opportunity to respond to your February 13, 2019, request to provide feedback on the collection, use and protection of sensitive consumer information. The ABA is the voice of the nation’s \$17.9 trillion banking industry, which is comprised of small, midsized, regional and large banks. Together, these institutions employ more than 2 million people, safeguard \$14 trillion in deposits and extend more than \$10 trillion in loans. Our members have a substantial interest in privacy and protecting sensitive consumer information, and we look forward to working with you and the Members of the Committee on this very important issue.<sup>1</sup>

## **Introduction**

In your request for feedback you asked five specific questions about how personally identifiable information is collected, used and protected and what might be done through legislation, regulation or best practices to give consumers more control over their personal information and otherwise improve the existing legal and regulatory environment. For example, your questions focus on data protection and consumer notice, adequate notice to consumers

---

<sup>1</sup> The views expressed in this letter are consistent with our joint responses with other financial trade groups to requests for information from the Administration regarding the protection of consumer privacy. The Associations’ comments to the National Telecommunications and Information Administration (NTIA) can be found here: [https://www.ntia.doc.gov/files/ntia/publications/financial\\_trades\\_ntia\\_comment\\_letter\\_nov\\_8\\_2019.pdf](https://www.ntia.doc.gov/files/ntia/publications/financial_trades_ntia_comment_letter_nov_8_2019.pdf)  
The Associations’ comments to the National Institute of Standards and Technology (NIST) can be found here: [https://www.nist.gov/sites/default/files/documents/2019/02/04/bpi-aba-sifma\\_bpi-aba-sifma\\_508.pdf](https://www.nist.gov/sites/default/files/documents/2019/02/04/bpi-aba-sifma_bpi-aba-sifma_508.pdf)

about the information that is being collected about them and the purpose of that collection and more consumer control over how information is shared with the financial regulators and private sector entities. You have also asked questions about credit bureaus and data brokers and related consumer protection issues. Because of the overlapping nature of these questions, and the fact that not all of the issues are directly relevant to ABA members, the following addresses these issues in a holistic manner, rather than question by question. We are very happy to provide more details and any other information at your request.

As a threshold matter, it is important to note that the current debate over privacy stems from concerns expressed by consumers and Members of Congress over how personal information is being used by social media platforms, data companies and others that monetize consumer information, as well as the security of sensitive information held by a broad range of non-bank entities. Given this new focus, it is important to stress that financial institutions have been subject to privacy and data protection rules for over 20 years, maintain robust internal systems designed in compliance with those rules, and are additionally subject to stringent federal and state regulatory oversight far beyond what is present for any other private, or even government sector entities. In enacting these financial privacy laws, Congress has taken a careful and balanced approach that protects the privacy interests of consumers, while ensuring that the financial system can still function effectively and provide the innovative products and services that consumers and businesses want and need.

As the Committee looks more deeply into the new challenges faced in what is now a rapidly evolving marketplace, we would encourage the Committee to continue to explore that balance of privacy protection and marketplace efficiency, so that the United States may remain competitive in the global market. Moreover, the Committee should consider how legislation can most effectively address the protection of individuals' privacy and safeguarding of their data, particularly in the context of advancing technology, and expanding menu of financial products and services offered by Fintech and other non-bank entities.

## Elements of Privacy Legislation

The U.S. financial sector is subject to a number of federal laws that 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. 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 greater detail, we do not believe that the California Consumer Privacy Act or the European Union's General Data Protection Regulation are good models for federal legislation for the financial industry. 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.
- **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 or state 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.

## 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”).<sup>2</sup>

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 disclosure practices and a 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 Bureau of Consumer Financial Protection (the “Bureau”). The Bureau’s model template is designed to follow the same easy-to-understand format used for nutrition labeling on food products, and was

---

<sup>2</sup> *See*, [http://uscode.house.gov/view.xhtml?req=\(title:15%20section:6801%20edition:prelim\)](http://uscode.house.gov/view.xhtml?req=(title:15%20section:6801%20edition:prelim))

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 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 to its limitations on sharing information with nonaffiliated third parties. These 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. These functions and activities depend on the flow of financial information where appropriate 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).

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 FinCEN about suspicious activities. Notwithstanding these exceptions, 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.

In addition to the GLBA, 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). And 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.

In addition, 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.

## **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.<sup>3</sup> 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 we 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. 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.

---

<sup>3</sup> 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/>

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.

Many non-bank fintech products rely heavily on consumer financial records held by financial institutions and some consumers want to use and share their data to access these applications. This process is often facilitated by data aggregators or “screen scrapers,” who collect this data from financial institutions and share it with third-party fintech providers. We support customers’ ability to share this data so long as consumers receive the same protection they receive from their financial institutions. In 2017, ABA outlined its principles for data financial data access, which include ensuring that consumers receive bank-level security, transparency and control whenever they share their sensitive financial data.<sup>4</sup> Our industry has been driving efforts to create secure standards that allow data to be shared in a way that protects consumers. One example of this is the Financial Data Exchange, LLC which has been set up to bring together technology companies and financial institutions to develop technology that will allow consumers flexibility to share their financial data in a way that gives them security, transparency and control over their data.<sup>5</sup>

---

<sup>4</sup> See, <https://www.aba.com/Advocacy/commentletters/Documents/ABA-Comment-CFPB-Data-Aggregators.pdf>

<sup>5</sup> The Financial Data Exchange (FDX) is nonprofit industry-led collaboration dedicated to unifying the incumbent and new entrant financial industry players around a common, interoperable, royalty-free standard that allows consumers and businesses to share their data without the sharing or storing of login credentials with third parties. FDX is made up of financial institutions, financial data aggregators and users of consumer permissioned data. FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC). <https://financialdataexchange.org/>

On a related issue, ABA members as well as policymakers have expressed concerns about the protection of consumer data held by other types of third parties, such as credit bureaus, in the wake of the Equifax breach. Standards that apply to financial institutions should extend to the third parties that received data from financial institutions. In that context, it is very important to consider the fact that the accuracy of data in consumer reports has been of vital importance both for consumers and consumer financial markets. Accurate consumer reports expand consumer access to credit and reduce the cost of credit to consumers and credit risk to lenders. Consumer reports also help lenders make decisions about whether to grant credit based on an applicant's ability to pay and to price credit based on the applicant's risk. It is in everyone's interest -- consumers, consumer reporting agencies, furnishers of information and users of consumer reports -- that our credit reporting system is based on accurate and complete information. Nonetheless, policymakers should be cautious about imposing new or different obligations under the FCRA without carefully evaluating the unintended consequences and ensuring that any changes would not dilute the effectiveness and use of consumer reports in a way that would ultimately harm consumers or that would discourage companies from furnishing data.

Finally, ABA members are growing increasingly concerned about the privacy and security of sensitive data financial institutions may share with government agencies, and which may later then be released to the public. In particular, new Home Mortgage Disclosure Act (HMDA) rules require the collection and public release of even more detailed mortgage loan statistics than under preexisting law. While the information is being released under the guise of public service, it could easily compromise consumer privacy. Government agencies have been, and will continue to be prime targets for state-sponsored actors, organized criminal groups, and hackers. Malicious actors have already compromised several massive government databases, which, in each instance, has resulted in the breach of millions of personal records. Government data security standards must be improved. But in the meantime, the HMDA data collection requirements and public "data dumps" could have adverse and unforeseen consequences for

consumer privacy and the credit markets. We urge the Committee to closely examine the scope and potential impact of these policies.

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.<sup>6</sup>

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”).<sup>7</sup> 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

---

<sup>6</sup> <https://ithandbook.ffiec.gov/>

<sup>7</sup> 15 U.S.C. § 6805(a).

this regard, Section 8 of the FDIA<sup>8</sup> 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.

As a consequence, 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.

---

<sup>8</sup> 12 U.S.C. § 1818.

#### **IV. Clear Preemption**

Any privacy legislation considered by Congress must eliminate the current inconsistent patchwork of state laws on privacy and data security. There is concern that if Congress does not enact uniform national privacy standards, the states will enact a patchwork of disparate and inconsistent requirements, resulting in further complexity and uneven protection for consumers. For example, in 2018, California enacted a significant new privacy law, the California Consumer Privacy Act (CCPA), prompted by an at-the-time pending ballot initiative. As a result, 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 must be disclosed to provide consumers with the goods and services that they need or request, and lacks the careful balancing and exceptions to allow information sharing that is inherent in the GLBA and its standards for financial institutions.

It is important to note, however, that the California legislature did recognize the privacy protections provided by the GLBA within the financial sector and therefore included a GLBA exception, acknowledging that banks and other financial institutions are already subject to federal privacy laws and already implement significant measures to protect consumers' privacy rights. However, concerns remain. The reach of the new law is very broad and will be subject to interpretation in implementing regulations and litigation and its full impact is still uncertain. For instance, banks outside of California could be required to expend considerable resources complying with a law with extraterritorial reach that affects only a portion of their customer base. The law also includes a provision that allows consumers to request that their information be deleted. Although there are exceptions, concerns remain that it may compromise law enforcement efforts to combat fraud, money laundering and terrorist financing

Other states are already considering adopting privacy laws similar to, if not modeled on, the CCPA, with sufficient differences that will exacerbate the existing patch-work of inconsistent state privacy and data breach laws. In fact, in 2019, twelve states 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.<sup>9</sup> One major problem in some of these proposals is that the definitions of “consumer” and covered “personal information” are 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 (e.g., the business may be in one state, its vendor may be in another state and the consumer may be in yet another state), competing state privacy regimes are likely to provide inconsistent requirements for how that information is handled. In addition, this lack of harmonization risks subjecting many banks and other financial institutions that offer insurance products to multiple conflicting state regimes. While these laws may be well-intentioned, they may hamper the free flow of data needed to provide consumers and businesses with beneficial financial products and services and to process financial transactions.

The need for a uniform national standard with strong preemption is also evidenced by the growing body of international privacy standards such as the European Union’s (EU) General Data Protection Regulation (GDPR). 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 reduce the financial sector’s ability to serve its 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.

---

<sup>9</sup> Hawaii, Massachusetts, Maryland, Mississippi, North Dakota, New Mexico, New Jersey, New York, Rhode Island, Virginia and Washington. California is likely to amend the CCPA.

The GDPR also has extraterritorial reach that potentially impacts the operations of U.S. banks both internationally and in certain cases, domestically, and this make it challenging for purposes of compliance. For instance, if a bank has customers living, working, or studying abroad, including college students enrolled at an EU university, academia and U.S. service members and their families stationed overseas, it may be subject to GDPR restrictions. Due to these and other concerns, the GDPR could potentially reduce the availability of U.S. banking services to U.S. citizens living in Europe.

Almost a year after the GDPR compliance date, we also have the benefit of observing how the European approach has impacted the daily lives of EU citizens. While regulatory uncertainty associated with GDPR is well-documented, the GDPR has also led to reliance on unwieldy compliance methods which intrude on consumers' experiences and in some cases, deny their access to services entirely. In fact, the most prominent and distinguishing element of Europeans' internet experience post - GDPR is not an innovation or feature -- it is a cascade of redundant warnings and disclaimers which interfere with the seamless digital experiences consumers are demanding, especially on mobile devices. Further, companies must use cookies to track which users have acknowledged and consented to their sites' policies, which has been interpreted by some to conflict with an existing EU cookie privacy rule that was not harmonized prior to the GDPR compliance date. The result is that those EU users who choose to block cookies for privacy reasons receive the most frequent notices and face the most disruption to routine experiences like reading a digital newspaper. In the financial services context, added friction discourages customer engagement with crucial information that empowers them in making informed financial decisions and monitoring accounts. It is important that any U.S. legislation takes lessons from Europe and recognizes that consumers realize better outcomes when they are able to engage with their bank.

Rather than promote a GDPR-like model, U.S. policymakers should work toward increasing the global interoperability of privacy regimes to help 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 EU 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.

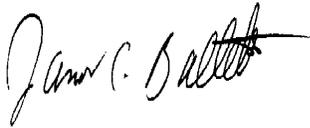
The increasing patchwork of state privacy and data breach laws must be replaced by a federal standard. The CCPA and GDPR, however, are not good models for the United States. In our view, it is critical that any new federal privacy law preempt existing state laws to avoid inconsistent and duplicative 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.

## 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.

Sincerely,

A handwritten signature in black ink, appearing to read "James C. Ballentine". The signature is written in a cursive style with a prominent horizontal stroke at the end.

James C. Ballentine