April 23, 2020

Harvey Perlman, Chair
William McGeveran, Reporter
Collection and Use of Personally Identifiable Data Committee
Uniform Law Commission
111 N. Wabash Ave
Suite 1010
Chicago, IL 60602

Dear Chairman Perlman and Reporter McGeveran:

The undersigned organizations[1] respectfully submit this comment for consideration by the Uniform Law Commission in response to the most recent draft of the proposed Collection and Use of Personally Identifiable Data Act ("Draft Act"). We appreciate the opportunity to participate and provide input on the latest draft. In addition, we would be happy to discuss the following suggested change or provide additional relevant material at your convenience.

[1] ABA (American Bankers Association) is the voice of the nation's $18.6 trillion banking industry, which is composed of small, regional, and large banks. Together, America's banks employ more than 2 million men and women, safeguard $14.5 trillion in deposits, and extend more than $10.5 trillion in loans.

The Consumer Bankers Association (CBA) partners with the nation's leading retail banks to promote sound policy, prepare the next generation of bankers, and finance the dreams of consumers and small businesses.

Credit Union National Association represents America's credit unions and their 115 million members.

The Independent Community Bankers of America® is dedicated exclusively to representing the interests of the community banking industry and its membership and creates and promotes an environment where community banks flourish. With more than 50,000 locations nationwide, community banks constitute 99 percent of all banks, employ nearly 750,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5 trillion in assets, nearly $4 trillion in deposits, and more than $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.

The National Association of Federally-Insured Credit Unions (NAFCU) advocates for all federally-insured not-for-profit credit unions that, in turn, serve nearly 120 million consumers with personal and small business financial service products. NAFCU provides its credit union members with representation, information, education, and assistance to meet the constant challenges that cooperative financial institutions face in today's economic environment. NAFCU proudly represents many smaller credit unions with relatively limited operations, as well as many of the largest and most sophisticated credit unions in the nation. NAFCU represents 73 percent of total federal credit union assets, 52 percent of all federally-insured credit union assets, and 70 percent of all federal credit union member-owners. NAFCU's membership also includes over 190 federally-insured state chartered credit unions.

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly one million employees, we advocate for legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. With offices in New York and Washington, DC, SIFMA is the US regional member of the Global Financial Markets Association (GFMA).

The following comments are limited to Section 3 of the Act that focuses on Scope, and specifically the Gramm-Leach-Bliley Act, which addresses the impact of the Draft Act on financial institutions. The undersigned organizations reserve the ability to offer comments on other provisions in the Draft Act during further deliberations of the drafting committee, including the section providing a private right of action.

Our respective members are strong proponents of protecting consumer data and privacy, and have been subject to extensive federal privacy and data protection laws and regulations for decades. As a threshold matter, we appreciate the inclusion of an exception for information subject to Title V of the Gramm-Leach-Bliley Act ("GLBA") in the second release from the Committee. The recognition of one of the existing privacy frameworks to which financial institutions are subject under federal law is an important improvement to the Act. Nonetheless, limiting the exception to information subject to the GLBA (as opposed to entities subject to the GLBA) ignores the carefully constructed financial privacy regime enacted by Congress that provides an effective and successful balance between strong consumer protections and ensures that consumer financial transactions take place in a safe and secure environment. As such, the current exception should be expanded to include entities subject to the GLBA.

Section 3. Scope

GLBA Exception

The Drafting Committee should amend section 3(b)(4) to expand the current exception provided for information subject to the GLBA to include an exception for financial institutions subject to the GLBA. Going forward, an exception for financial institutions subject to the GLBA should be included in any privacy legislation enacted by the states. In furtherance of this effort, the undersigned organizations recommend section 3(b)(4) of the Draft Act be amended to read:

> *A financial institution subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §6801 et seq.), and the implementing regulations promulgated thereunder.*

GLBA Provides Strong Consumer Protections

The GLBA mandates two major protections: (i) comprehensive information security requirements and (ii) privacy notice obligations and information sharing restrictions. 15 U.S.C. §§ 6801 *et seq*. The GLBA requires financial institutions to establish an information security program that protects customer information through administrative, technical and physical safeguards. Each program must be designed so as to ensure the security and confidentiality of customer information, protect against any foreseeable risks, protect against its unauthorized access or use, and ensure its proper disposal. The GLBA contains strict security and confidentiality requirements for consumer information and requires that financial institutions thoroughly investigate incidents of unauthorized access to, or use of, personal information and notify impacted individuals if misuse of their personal information is reasonably possible.

The GLBA's various privacy obligations and limitations apply with respect to "nonpublic personal information" relating to a "consumer." For purposes of the GLBA, a "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family or household purposes. *See* 12 C.F.R. § 1016.3(e)(1). And, "nonpublic personal information" includes any information:

(1) "[a] consumer provides to [a financial institution] to obtain a financial product or service from" the financial institution;
(2) "[a]bout a consumer resulting from any transaction involving a financial product or service between" the financial institution and the consumer; or
(3) the financial institution "obtain[s] about a consumer in connection with providing a financial product or service to that consumer."

12 CFR §§ 1016.3(p)(1) (definition of "nonpublic personal information"), 1016.3(q)(1) (definition of "personally identifiable financial information").

With respect to privacy, among other things, the GLBA imposes significant limitations on the ability of a financial institution to disclose "nonpublic personal information" relating to a "consumer" to a nonaffiliated third party. Specifically, the GLBA prohibits a financial institution from disclosing "nonpublic personal information" about a "consumer" to a nonaffiliated third party unless: (1) the institution has provided the consumer with notice and an opportunity to opt out of the disclosure of her information and the consumer has not opted out; or (2) an exception applies that permits the financial institution to disclose the information. *See* 12 C.F.R. § 1016.10.

The GLBA also imposes reuse and re-disclosure limitations on persons that receive "nonpublic personal information" from a financial institution, such as a financial institution's service provider, or a nonaffiliated third party to whom a financial institution is permitted to disclose information under an exception. For example, a financial institution that will disclose "nonpublic personal information" to a nonaffiliated third party in order for the third party to perform a service or function on behalf of the financial institution must, among other things, "[e]nter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which [the financial institution] disclosed the information." 12 C.F.R. § 1016.13(a)(1). Separate from service provider relationships, if a financial institution discloses "nonpublic personal information" to a nonaffiliated third party under an exception (*e.g.*, for fraud prevention purposes), the nonaffiliated third party, among other things, only "may disclose and use the information pursuant to an exception . . . in the ordinary course of business to carry out the activity covered by the exception under which [it] received the information." 12 C.F.R. § 1016.11(a)(1). As a result, if a person receives protected information from a financial institution, that person generally only may use the information for the purpose for which it received the information (*e.g.*, to perform services for the financial institution) or another purpose permitted by the GLBA.

The GLBA also imposes obligations that a financial institution provide notice of its privacy practices to consumers in various contexts. For example, the GLBA requires that a financial

institution provide a "clear and conspicuous notice that accurately reflects [the financial institution's] privacy policies and practices to," among others, any "individual who becomes [the financial institution's] customer, not later than when" the financial institution establishes the customer relationship with the individual. 12 C.F.R. § 1016.4(a)(1). For purposes of this obligation, a "customer" is a "consumer" who has "a continuing relationship" with a financial institution in which the financial institution provides "one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes." 12 C.F.R. §§ 1016.3(i) (definition of "customer"), 1016.3(j)(1) (definition of "customer relationship"). Moreover, except in certain instances, a financial institution is required to provide its privacy policy to a customer "not less than annually during the continuation of the customer relationship." 12 C.F.R. § 1016.5(a)(1).

GLBA is Carefully Crafted to Ensure Compliance with Existing Law

The GLBA includes carefully crafted exceptions to its restrictions on sharing information with nonaffiliated third parties to ensure financial institutions can maintain, process and service the accounts, payments, transactions and other financial activities that consumers expect. Exceptions to the notice and opt out requirement encompass sharing for purposes of completing transactions, servicing an account, fraud prevention, ensuring compliance with other legal and regulatory mandates, responding to legal process, and in accordance with a joint marketing arrangement with another financial firm. These exceptions were carefully created to ensure that financial markets function properly, that financial institutions are able to provide consumers with the products and services that they expect, and that financial institutions can comply with legal mandates and help protect against fraud.

Other Federal and State Financial Privacy Laws

It is also important to note that the GLBA is not the only U.S. privacy law regulating financial institutions. For example, the federal Right to Financial Privacy Act ("RFPA") generally prohibits a financial institution from disclosing customer information to the U.S. federal government, except in specified contexts and then only in accordance with the procedural requirements of the statute. *See* 12 U.S.C. § 3401 *et seq*. In addition, the federal Fair Credit Reporting Act ("FCRA") regulates the disclosure of, access to and use of "consumer reports," sharing of information among affiliated financial institutions and the use of information shared among affiliates for marketing purposes *See* 15 U.S.C. § 1681 *et seq*. Moreover, various states have their own laws that are similar to the GLBA, RFPA and FCRA, such as the California Financial Information Privacy Act. *See, e.g.*, Cal. Fin. Code § 4050 *et seq*.

Depository Institutions are Subject to Strict Federal Oversight and Examination

Special consideration should be given to the ongoing supervision and oversight of bank holding companies and depository institutions subject to GLBA. A key distinction that sets the federal regulators' GLBA oversight apart from the mere "enforcement" of other state privacy and security requirements is the routine monitoring and testing of bank holding companies and depository

institutions' compliance with GLBA requirements. Regulatory agencies regularly examine such institutions' compliance with laws and regulations through full-scope, on-site examinations. In addition, examiners are permanently placed on-site at offices of certain large depositories. Federal depository regulators even conduct regular GLBA compliance examinations of some large service providers to financial institutions under the Bank Service Company Act, 12 USC 1861-1867(c). This oversight by federal depository regulators helps create an environment of accountability and ensures that any problem areas are addressed expeditiously. Furthermore, if a depository institution fails to comply with GLBA, the federal depository institution's regulators can bring enforcement actions to ensure that GLBA's privacy and information security mandates are swiftly implemented. What is important to recognize, though, is that depository institutions are subject to a pro-active compliance regime as opposed to an enforcement regime that comes into play after consumer harm may have already occurred.

Conclusion

In conclusion, and in recognition of the robust legal and regulatory privacy framework financial institutions are subject to, we strongly urge the Drafting Committee to adopt the proposed language revising the Draft Act's GLBA exception so that it is not limited to information subject to the GLBA, but instead exempts financial institutions subject to the GLBA. A provision solely including an information-level GLBA exception would create confusion and additional compliance headaches without providing meaningful consumer protection or benefits. Additionally, without an entity-level exception, laws that follow an information-level exception framework could inadvertently facilitate unauthorized access to sensitive personal information about consumers. Because of this threat, financial institutions should be exempt from laws that allow a consumer to request access to sensitive information. A full financial institution exemption will allow financial institutions to instead focus on compliance with the existing federal and state financial privacy frameworks and improving meaningful consumer protections while ensuring the proper function of financial markets.

Again, we greatly appreciate the Drafting Committee's consideration of our recommendation. We look forward to continued discussion and participation in the drafting process.

Sincerely,

American Bankers Association
Consumer Bankers Association
Credit Union National Association
Independent Community Bankers Association
National Association of Federal Credit Unions
Securities Industry Financial Markets Association