

December 10, 2020

Harvey Perlman, Chair  
Jane Bambauer, 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 Bambauer:

The American Bankers Association and the undersigned state bankers associations, representing banks of all sizes, respectfully submit this comment for consideration by the Uniform Law Commission. We appreciate the opportunity to provide input on the Committee's draft and respond to recent comments targeting our industry.

The most recent draft of the Collection and Use of Personally Identifiable Data Act contains an exception for information subject to the federal Gramm-Leach-Bliley Act ("GLBA"). Similar to other state laws, such as the California Consumer Privacy Act, this exception was included in the Act because the committee recognized that federal law provides significant consumer protections for bank customers and that a state privacy law should not disrupt this carefully balanced approach. In recent comments, one group, whose members are not subject to federal privacy law or regulation regulating their industry and are not subject to examination by federal regulators with respect to their privacy and data security practices, has argued for the removal of the compromise approach supported by the Committee related to GLBA. We strongly oppose this.

Their comments fail to mention that banks are heavily regulated and supervised entities and misstates several key data privacy protections that the GLBA provides. The GLBA not only mandates disclosure of privacy practices and information sharing restrictions, but it further requires financial institutions to establish an information security program that protects customer information. Each program must be designed 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 also imposes significant limitations on the ability of a financial institution to disclose "nonpublic personal information" relating to a "consumer" to a nonaffiliated third party, and 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 (*e.g.*, for fraud prevention purposes). As a result, if a person receives protected information from a financial institution, that person generally may only 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. That is, the GLBA's protections follow the information.

As mentioned, a key distinction that sets the federal regulators' GLBA oversight apart from the "enforcement" regime applied by other privacy and security requirements, is the standard and routine auditing of bank holding companies' and depository institutions' compliance with not only GLBA requirements but also those mandated by other federal laws, including other federal privacy laws. Also significant is the fact that the federal banking agencies regularly examine such institutions' compliance with these laws and regulations through full-scope, on-site examinations. Federal depository regulators also conduct GLBA compliance examinations of large bank service providers under the Bank Service Company Act, 12 USC 1861-1867(c). This oversight by federal regulators helps create an environment of accountability and ensures that any issues that may arise are addressed expeditiously. Further, if a depository institution fails to comply with the GLBA, the federal depository institution's regulators can bring enforcement actions to ensure that the GLBA's privacy and information security mandates are swiftly implemented. Overall, it is essential to recognize that depository institutions are subject to a proactive compliance regime, as opposed to an ad hoc enforcement regime that comes into play only after consumer harm may have already occurred.

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

Sincerely,

American Bankers Association  
Alabama Bankers Association  
Alaska Bankers Association  
Arizona Bankers Association  
Arkansas Bankers Association  
California Bankers Association  
Colorado Bankers Association  
Connecticut Bankers Association  
Delaware Bankers Association  
Florida Bankers Association  
Georgia Bankers Association  
Hawaii Bankers Association  
Idaho Bankers Association  
Illinois Bankers Association  
Indiana Bankers Association  
Iowa Bankers Association  
Kansas Bankers Association  
Kentucky Bankers Association  
Louisiana Bankers Association  
Maine Bankers Association  
Maryland Bankers Association  
Massachusetts Bankers Association  
Michigan Bankers Association  
Minnesota Bankers Association  
Mississippi Bankers Association

Missouri Bankers Association  
Montana Bankers Association  
Nebraska Bankers Association  
Nevada Bankers Association  
New Hampshire Bankers Association  
New Jersey Bankers Association  
New Mexico Bankers Association  
New York Bankers Association  
North Carolina Bankers Association  
North Dakota Bankers Association  
Ohio Bankers League  
Oklahoma Bankers Association  
Oregon Bankers Association  
Pennsylvania Bankers Association  
Puerto Rico Bankers Association  
Rhode Island Bankers Association  
South Carolina Bankers Association  
South Dakota Bankers Association  
Tennessee Bankers Association  
Texas Bankers Association  
Utah Bankers Association  
Vermont Bankers Association  
Virginia Bankers Association  
Washington Bankers Association  
West Virginia Bankers Association  
Wisconsin Bankers Association  
Wyoming Bankers Association