August 28, 2025

The Hon. French Hill
Chairman
Committee on Financial Services
United States House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

The Hon. Andy Barr
Chairman
Subcommittee on Financial Institutions
Committee on Financial Services
United States House of Representatives
2430 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Hill and Chairman Barr:

On behalf of the financial trade associations listed below, please see the accompanying submission in response your Request for Information (RFI) on the state of current federal consumer financial data privacy law. In addition, the joint trades welcome the opportunity to provide feedback on your request for legislative proposals to account for changes in the financial services sector.

The attached response to the RFI is based on initial feedback from our collective member institutions. Given the complexity of these issues and the measure of their potential impact on the financial services industry, we look forward to providing additional feedback on this topic as we receive it from our members and continuing to work with you as the Committee's work progresses.

Thank you for the opportunity to provide feedback on your RFI on federal consumer financial data privacy law.

Sincerely,

American Bankers Association
America's Credit Unions
Bank Policy Institute
Consumer Bankers Association
Securities Industry and Financial Markets Association

Joint Financial Trades Response to the

House Financial Services Committee

Request for Information

Current Federal Consumer Financial Data Privacy Law and

Potential Legislative Proposals

August 28, 2025

Chairman Hill and Chairman Barr, we appreciate the opportunity to respond to the Request for Information[1] (RFI) issued by the House Financial Services Committee as it assesses the current federal consumer financial data privacy law and considers appropriate legislative efforts to account for changes in the consumer financial services sector. This letter can be viewed in conjunction with comment letters filed with the House Energy & Commerce Committee on data privacy issues.[2]

Cumulatively, the assembled joint trade associations (the American Bankers Association, America's Credit Unions, the Bank Policy Institute, the Consumer Bankers Association, and the Securities Industry and Financial Markets Association; see Appendix A for additional information) represent members comprising the vast majority of financial institutions with decades of experience being supervised for compliance with the Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), and other consumer privacy laws. They are also well acquainted with related issues such as permissioned data sharing (sometimes referred to as open banking) as well as compliance with the emerging patchwork of state privacy laws.

Further, although not expressly asked, the Committee should consider including data breach notification into its drafting. In addition to federal data breach notification requirements, complying with 50 inconsistent state data breach notification requirements plus the District of Columbia and other territories is overly burdensome on financial institutions and provides little if any value for consumers, as notice to impacted customers is already covered by GLBA. We hope that the Committee will consider addressing this issue when considering amendments to federal privacy legislation.

Our feedback to the RFI questions is based on recent and ongoing conversations with our member organizations. We note that this feedback is preliminary in nature and look forward to continuing productive discussions with Committee members and staff in this essential domain.

[1] https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=410833.

[2] See https://www.aba.com/advocacy/policy-analysis/joint-trades-letter-to-commerce-committee-on-data-privacy (April 4, 2025) and https://www.aba.com/advocacy/policy-analysis/Joint-supplemental-letter-regarding-data-privacy-bill (August 19, 2025).

Overall, we believe:

- GLBA is a carefully calibrated regime designed to avoid interference with core financial activities that benefit consumers, and will continue to be the most appropriate vehicle to address data privacy for financial institutions;

- The Committee should play an essential role in discussions on federal privacy legislation given its expertise in financial services, including any discussion of amendments to GLBA (e.g., additional data subject rights with appropriate exemptions and tailoring based on the unique fraud, security, and other risk considerations relevant to financial services);

- GLBA should have strong preemptions for state privacy laws; moreover entities, affiliates, and data subject to GLBA must be exempt from any comprehensive federal consumer privacy laws in order to avoid interference with the GLBA and important financial activities such as fraud prevention and underwriting;

- GLBA should continue to be enforced by federal regulators rather than through private litigation;

- GLBA should be amended to create a more consistent regulatory playing field among traditional and novel financial institutions as well as other entities operating in the financial ecosystem;

- GLBA should be amended to include a safe harbor for the sharing of information regarding fraud and scams; and

- GLBA should be harmonized with Section 1033 of the Dodd-Frank Act as appropriate, including to apportion liability for when consumer-permissioned data sharing results in a data breach as well as part of the data subject rights issue.

Please see our initial responses to each of the RFI questions below.

1. Should we amend the GLBA or consider a broader approach?

GLBA is evergreen and continues to function well for supervised financial institutions and in protecting consumers. GLBA was carefully crafted to provide consumers with meaningful privacy rights and transparency, while avoiding interference with financial institutions' ability to offer high-quality financial products that allow consumers to make payments and bank confidently.

Financial institutions use data in unique (and often legally mandated) ways compared to other sectors, including to protect against fraud, money laundering, terrorist financing, and other illicit

activities. They also use data to facilitate superior underwriting decisions that take into account non-traditional creditworthiness metrics, thus enabling financial institutions to extend credit to underserved communities and new markets.

As a framework built for financial institutions, GLBA is carefully calibrated to avoid restricting these crucial activities, while allowing consumers to broadly exercise their privacy choices over disclosures to nonaffiliated third parties. Moreover, GLBA provides federal financial regulators with meaningful authority to adopt implementing regulations and closely supervise financial institutions—ensuring that the regime has adapted, and will continue to adapt, over time as privacy considerations evolve. Our members are confident that, particularly with the close supervision of their federal financial regulators, the GLBA compliance regime will continue to provide consumers with strong protections over the coming decades as it has since 1999.

Of course, our members recognize the significant technological and societal changes that have occurred since the passage of GLBA, such as the increasing digitization of banking and financial markets, the rise of fintech and data brokers, entrenchment of service providers, and proliferation of comprehensive state laws.

As Congress considers additional legislation to protect consumer privacy in this shifting world, it may be considering the merits of a comprehensive federal privacy bill. However, the application of comprehensive privacy laws—including any new federal privacy law and existing state privacy laws like the California Consumer Privacy Act of 2018, as amended[3] (CCPA)—to financial institutions creates a cumbersome patchwork while being ill-suited to operational realities and the unique challenges of personal data processing for financial institutions.

Targeted amendments to GLBA would allow House Financial Services to take into account the unique circumstances of financial institutions and how they process, share, and use data to ensure a safe & sound payments and banking system for consumers—whereas federal comprehensive privacy legislation would presumably seek to address the privacy risks associated with entities with very different data usage and potential privacy harms (e.g., tech companies). The requirements that may be appropriate for other sectors risk interfering with core financial activities, such as payment network activities, underwriting, and fraud prevention.

2. *Should we consider a preemptive federal GLBA standard or maintain the current GLBA federal floor approach?*

Any update of GLBA should include a preemptive federal standard for all laws governing privacy notices, consumer rights, and the processing of personal information for financial institutions. The federal floor approach has led to consumer/business/agency confusion, increased regulatory burden, and an unstable environment for interstate commerce.

---

3 https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Strong preemption of state banking-specific privacy laws is essential in order to avoid inadvertent limitations on core banking activities as well as conflicting requirements for certain activities. For example, joint marketing under California's banking-specific privacy law can create tension with the federal approach under GLBA, and there are a number of requirements under California's comprehensive privacy law (CCPA) that are duplicative or even conflicting with the GLBA (e.g., prescriptive cyber audit and risk assessment requirements).

As another example, there is also a challenge associated with sector-specific requirements for insurance companies, many of which are affiliates of financial institutions. Insurers or insurance entities that are affiliates of financial institutions have singular, additional risks and costs since the current form of GLBA delegates rulemaking power to the states. As states continue to act under the status quo, financial institution-owned insurance entities are subject to an even greater level of risk and compliance issues due to dual regulation because of their status and organization as: a) an insurance entity; and b) as an entity owned by a parent financial institution.

There have also been challenges where state laws intrude on areas regulated under federal law (e.g., the Fair Credit Reporting Act). Preemption would enable national consistency and stability, avoid state intrusion on federal laws, ensure that federal regulators are able to regulate national banks without interference, and reduce undue compliance costs. If financial institutions are forced to balance federal and state requirements in designing their privacy programs, they will continue to face challenging questions of how to address duplicative and even conflicting requirements that can undermine the robust GLBA compliance expected by their federal regulators.

3. If GLBA is made a preemptive federal standard, how should it address state laws that only provide for a data-level exemption from their general consumer data privacy laws?

Enacting federal legislation only makes sense if it codifies strong preemption of these state laws. As can be seen in a supplemental letter to the House Energy & Commerce Committee,[4] the current patchwork approach is onerous for both consumers and financial institutions without corresponding benefit to consumer privacy. For example, consumers need to review two distinct sets of disclosures since the requirements of CCPA and GLBA generally cannot be reconciled in one notice, and they have to take separate steps to exercise rights under both sets of laws rather than exercising rights in a streamlined manner. For convenience, we are reproducing the anecdotes our members provided regarding associated compliance burden in Appendix B. While the data-level exemption in California creates the most issues given financial institutions' overlapping use of both GLBA and non-GLBA data, even states with entity-level exemptions inject unnecessary risk into the environment.

We encourage the House Financial Services Committee to work with the Energy & Commerce Committee to ensure that any new or revised federal framework for data privacy (including

[4] https://www.aba.com/advocacy/policy-analysis/Joint-supplemental-letter-regarding-data-privacy-bill (August 19, 2025).

GLBA) supersedes the patchwork of state law, thereby affirming Congress' leadership in this vital area and creating a uniform national standard that provides consistent consumer protections.

If comprehensive federal privacy legislation is passed and state law preemption is introduced into GLBA, GLBA could in turn incorporate some of the principles from the state laws, such as affording consumers additional data subject rights. However, any such processes must be carefully balanced with existing information available to consumers in the banking context and include appropriate exemptions and tailoring for financial institutions' unique data processing activities, as well as comport with consumer protection and safety & soundness obligations.

4. How should GLBA relate to other federal consumer data privacy laws, both a potential general data privacy law and current sector-specific laws?

GLBA should continue to apply to information collected, used, shared, and retained from consumers in the context of providing financial services. We also note it has, and should continue to have, a strong information security component as well as sections relevant for engaging with nonaffiliated third parties.

As discussed above, if Congress proceeds with federal privacy legislation, an updated GLBA should supersede state consumer privacy laws (both those building on the current GLBA floor as well as comprehensive privacy laws) in their entirety. The meritorious concepts therein could be reflected in federal legislation as appropriate, either in GLBA for the broader financial services ecosystem or in a comprehensive privacy bill for other industries. There should be no duplicative or inconsistent provisions with existing legal requirements in either data privacy law. Moreover, both GLBA and the comprehensive privacy law should exclude employment matters as well as business data, which is consistent with the approach taken under GLBA and the majority of state privacy laws today and reflecting the distinguishable uses of data and harms in those contexts.

In addition, neither federal privacy legislation nor GLBA should include a private right of action, which can undermine the ability of federal regulators to drive appropriate practices through strategic enforcement. This is particularly true in the context of supervised financial institutions, which are very closely examined by their federal regulators as discussed elsewhere in this letter. A private right of action would also only serve to encourage frivolous litigation from plaintiffs' attorneys, such as the opportunistic lawsuits and copious demand letters stemming from ambiguous language in the current text of the California Invasion of Privacy Act. In these suits, companies can be forced to settle to avoid outrageous litigation costs even when the company is not at fault.

Finally, to give an example of the kinds of amendments that could be uniquely considered for GLBA as compared to a comprehensive privacy law, GLBA could be amended to include a safe harbor for the sharing of information regarding fraud and scams. Today, financial institutions can be limited in their ability to share information, both with each other and with law enforcement, which hampers both government and industry efforts to prevent bad actors and better protect consumers. Our members have seen great success in combatting money laundering and terrorist

financing when industry and the government can work hand in hand, and such an amendment would facilitate this.

a. *Should GLBA "financial institutions" be subject to entity-level or data-level exemptions from these laws?*

Any federally supervised financial institution subject to the GLBA should be exempted at the entity, affiliate, and data level from other state and federal privacy laws. At the same time, GLBA could potentially be amended to extend a supervisory regime to other types of financial institutions as discussed further below.

5. How should we define "non-public personal information" within the context of privacy regulations?

The GLBA definition of "nonpublic personal information" continues to be appropriate and properly captures the scope of consumer data that is collected, disclosed, or otherwise processed by financial institutions in the course of providing consumer financial products and services.

For any comprehensive federal privacy legislation, many of the comprehensive state privacy laws have definitions that could be leveraged for sectors outside the financial services ecosystem (e.g., information that is linked or reasonably linkable to an identified or identifiable natural person, excluding deidentified data or publicly available information).

a. *Does the term "personally identifiable financial information" in GLBA require modification?*

Expansion of the scope of non-public personal information/personally identifiable financial information would only be appropriate in the context of state law preemption being introduced into the statute. The scope of GLBA works well today, and expansion is not necessary for the statute to function well as designed. If Congress does revisit the definition, the current concept could be amended to include additional data points, such as those on prospective customers, certain non-consumer accounts, and customer counterparties.

6. Do the definitions of "consumer" and "customer relationship" in GLBA require modification?

Today, the requirements of GLBA are appropriately calibrated to the very different circumstances of a consumer and a customer. For example, financial institutions interact and use data very differently for a consumer who engages in an isolated ATM transaction, as compared to a customer with whom they have a banking relationship. It would not be possible to meet the requirements of the GLBA for customers if they were applied to consumers (e.g., providing an annual privacy notice to a consumer who once used an ATM.)

Accordingly, while there could be an opportunity to streamline these terms, this would need to be accompanied by a careful reassessment of the associated GLBA obligations to avoid breaking the current framework and creating impossible or unduly burdensome obligations.

7. Does the current definition of "financial institution" sufficiently cover entities that should be subject to GLBA Title V requirements, such as data aggregators?

As background, the regulatory playing field is not entirely consistent today for traditional financial institutions (e.g., banks and credit unions) and more novel financial institutions (e.g., fintechs). For example, the rise of digital assets and the crypto ecosystem represent a new way for consumers to obtain financial products and services—but the applicability of GLBA is not always clear or enforced for some of the players in this ecosystem.

Another differentiator among financial institutions is their level of supervision by federal regulators. Banks, credit unions, and their affiliates are heavily supervised by regulators, while some other financial institutions (e.g., fintechs) may not be subject to the same oversight. Prudential regulators are well-positioned to assess: a) data privacy controls to prevent unauthorized monetization; b) information security programs to safeguard from data breaches; and c) appropriate fraud prevention activities, among others. Supervision by these regulators also ensures financial institutions' privacy protections stay up-to-date, even in the absence of legislative change.

One option would be to clarify the definition of "financial institution" through an amendment to expressly include categories such as fintechs, financial data aggregators, and certain crypto companies to enshrine the concept of same activity, same risk, same regulation, and same supervision. Those entities should be subject to comparable federal examination programs and enforcement mechanisms as other financial institutions. Alternatively, a separate category of personal financial data holders could be created to ensure that rigorous data protection requirements are imposed on such entities even if they are not defined as "financial institutions."

Consistent with the above, these companies should undergo a comparable oversight regime for their privacy and information security practices. As things currently stand, at the federal level many are subject only to ***enforcement*** by the Federal Trade Commission (FTC) or the Consumer Financial Protection Bureau (CFPB)—which is far lighter than the ongoing and rigorous supervisory regime in place at members of the undersigned. This distinction is particularly important for information security purposes and the associated issue of data breach notification requirements, including notice to a federal agency conducting examinations.

8. Are there states that have developed effective privacy frameworks?

We speak only insofar as the frameworks pertain to the financial services ecosystem—no. By its very nature, a patchwork of privacy laws is problematic because so many businesses operate on an interstate level. Consumers are inundated by a variety of specific disclosures and banners, designed to meet different state expectations, and may be confused by the differing availability

of consumer rights and other protections across states. While we appreciate the spirit that motivates the passage of these laws, the continuous burden imposed on businesses is not offset by corresponding benefit to consumers.

a. Which specific elements from these state-level frameworks could potentially be adapted for federal implementation?

Certain disclosures (particularly around data collection and usage) and data access rights are all elements that could reasonably, with careful application and tailoring, be considered for updates to GLBA as well as comprehensive federal privacy legislation. It will be essential to tailor any new data access rights for GLBA to the unique circumstances of financial institutions that are discussed in response to other questions above (e.g., ensuring that financial institutions are not required to provide data to bad actors).

Any deletion rights must be meticulously evaluated due to the critical importance of records for various legal and business needs. Further, the right to correct probably would not translate well to a GLBA amendment since financial institutions generally offer the ability to customers to update and correct personal information through normal account management processes, are incentivized to do so, and are subject to existing Fair Credit Reporting Act requirements.

9. Should we consider requiring consent to be obtained before collecting certain types of data, such as PIN Numbers and IP addresses?

No. A consent-based framework is not appropriate for federally-regulated financial institutions. This type of framework risks interfering with financial institutions' ability to collect data that is essential to provide requested financial products and services, prevent fraud, and otherwise protect consumers and the safety & soundness of the banking system. For example, an inability to collect a PIN Number could result in a financial institution being unable to confirm a customer's identity when they seek to withdraw funds and thus prevent a customer from obtaining their funds absent more invasive verification techniques. Similarly, an inability to collect IP addresses could undermine financial institutions' fraud detection and prevention programs because this information plays an essential role in those activities.

A consent-based regime can also result in consent fatigue for consumers that undermines the admirable goals of consumer choice, which can instead be achieved through an opt-out framework like that which already exists under the GLBA.

The greatest source of risk with collection of information often falls on certain data brokers and third parties crawling the web, which often do so in contravention of terms of service and misappropriate content for training AI models, building consumer profiles, or other pursuits. These sorts of situations should be covered by any federal legislation for entities outside the financial services ecosystem.

10. Should we consider mandating the deletion of data for accounts that have been inactive for over a year, provided the customer is notified and no response is received?

No. Under GLBA and the Interagency Guidelines Establishing Information Security Standards issued by their prudential regulators, banks and credit unions are already required to ensure the proper disposal of data through their documented information security program. Further SEC Regulation S-P, as amended, imposes data disposal and information security program requirements on broker-dealers, investment advisers and other SEC-regulated financial institutions. Given this, they already have appropriate data retention policies, making a prescriptive data deletion requirement unnecessary and in tension with financial institutions' legal obligations under their existing federal regulation.

Indeed, such a requirement would create serious compliance issues for highly regulated financial institutions. For example, this requirement could interfere with the ability to comply with reporting requirements and with state escheatment mandates. Moreover, there are codified retention periods for federal laws including but not limited to the Bank Secrecy Act, Electronic Funds Transfer Act, Equal Credit Opportunity Act, Truth in Savings Act, as well as various obligations for mortgage loan and servicing files. Many regulations have document retention requirements of two years or more. In addition, financial institutions have other legal obligations that rely on the usage of data; for example, Regulation E has obligations around error resolution, providing periodic statements for prepaid accounts, etc.

Finally, some account types and financial products are also designed to require very little customer engagement over time, so they may properly be dormant for extended periods (e.g., 10-year CDs, prepaid safe deposit box rental, or target date mutual funds). Reaching out to customers to confirm account details is not consistent with recommended business practices and risks teaching our customers to respond to unprovoked emails and phone calls from fraudsters claiming to be their financial institution confirming their account details before closing their account for inactivity.

Accordingly, a deletion mandate would prove unworkable to implement effectively without causing unintended consequences. Such a requirement would also be inconsistent with customer expectations, as customers do not expect to immediately lose crucial prior account and transaction data that could be important for their own purposes (e.g., litigation).

11. Should we consider requiring consumers be provided with a list of entities receiving their data?

No. Requiring financial institutions to provide a list of actual entities receiving consumer data would be highly burdensome to produce and maintain. Further, releasing this information could inadvertently expose trade secrets and/or confidential business information and discourage the use of alternative vendors for redundancy & resiliency purposes. Disclosing a service provider list can pose a security risk to the financial institution and the broader financial services ecosystem. While threat actors know that financial institutions have robust security programs, they may target vendors to obtain consumer financial data.

In addition, implementing such a requirement would require a mature data inventory/governance program, which is aspirational for many community and mid-size financial institutions at this time.

A more practical approach would be to require financial institutions to disclose ***categories*** of third parties, which would align with the standard contained in many comprehensive state privacy laws (for example, the CCPA). This would recognize the operational challenges and risks associated with identifying specific entities and instead focus on transparency through categorical disclosures. For awareness, HR 1165, introduced in the 118th Congress by former Chairman Patrick McHenry, initially contemplated the production of a list of entities but ultimately adopted a more feasible standard of "categories and types" of third parties.

12. Should we consider changing the structure by which a financial institution is held liable if data it collects or holds is shared with a third-party, and that third-party is breached?

Yes, any entity that holds consumer financial data should be held to the same data protection standards and held liable for the mishandling or misuse of such data regardless of whether the entity holding the data is a "financial institution" under GLBA or operating as part of the broader financial services ecosystem.

There is a clear and growing need for a legal/regulatory framework for liability of third and other downstream data recipients, particularly in the context of consumer-permissioned data sharing. Financial institutions do not have control over the third parties with which their customers engage (e.g., financial data aggregators and fintech apps) or the downstream entities receiving the data from these companies. These disclosures can occur without a financial institution's knowledge, even if a Data Access Agreement is in place.

Currently, liability and breach notification obligations are governed by bilateral contracts, which vary widely depending on a financial institution's market power and negotiation leverage. This fragmented approach introduces unnecessary risk in the financial services ecosystem and confusion for consumers. A more structured framework should include:

- Notification and indemnification protocols across the data-sharing chain (e.g., data provider, financial data aggregator, and data recipient); and

- Statutory obligations to investigate and identify the locus of the breach and/or matter in dispute.

Accordingly, in a parallel process to any discussions around GLBA amendments, the Committee may wish to amend Section 1033 of the Dodd-Frank Act to create more clarity around scope and obligations, or to consider revisions to its data access provisions. It may also consider taking the opportunity to sunset the dangerous practice of screen scraping, which is anathema to consumer privacy and security.

The existing regulation implementing Section 1033 of the Dodd-Frank Act[5] is flawed and exceeded Congressional intent. On August 22, 2025, the current CFPB leadership issued an Advanced Notice of Proposed Rulemaking to begin the process to substantially revise the flawed rule, including whether existing provisions addressing screen scraping are sufficient.[6] We urge Congress to monitor this process to ensure that any revised final rule implementing Section 1033 does not conflict with any updated data privacy laws that Congress enacts.

13. Should we consider changes to require or encourage financial institutions, third parties, and other holders of consumer financial data to minimize data collection to only collection that is needed to effectuate a consumer transaction and place limits on the time-period for data retention?

No. Data minimization requirements present unique issues for financial institutions compared to other types of entities. Financial institutions have long relied on diverse data sources to support fraud prevention, underwriting, and risk management—all of which are essential to protect consumers and the safety and soundness of the banking system and the financial markets. For example, data such as IP addresses or information shared across financial institutions via fraud consortiums can be pivotal in catching bad actors or preventing a consumer from being defrauded. These activities are essential to achieve socially beneficial goals, yet risk being undermined by the data minimization standard suggested by this question.

Indeed, requiring financial institutions to minimize data collection to include only data needed to effectuate a consumer transaction would introduce substantial ambiguity regarding permissible uses of such data for fraud prevention and other core compliance functions. It could also hinder innovation related to the development of AI and would place US financial institutions at a competitive disadvantage vis-à-vis foreign banks. Finally, as discussed above in response to Question 10, data retention limits are unnecessary given existing protections related to data disposal under the GLBA and Interagency Guidelines and banks' already robust data retention policies.

Further, broker-dealers and investment advisers have stringent record retention requirements under the Securities Exchange Act and the Investment Advisers Act which would potentially conflict with any mandated data destruction requirement.

The Committee should bear in mind that collection of data directly by first parties is fundamentally different than a third party retrieving the consumer's data from a financial institution pursuant to the consumer's authorization. The latter scenario is a distinct subset of financial activity and accordingly should have tailored obligations for the collection, use, and protection of personal information.

---

[5] *See* https://www.federalregister.gov/documents/2024/11/18/2024-25079/required-rulemaking-on-personal-financial-data-rights; *see also* https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title12-section5533&num=0&edition=prelim.

[6] https://www.federalregister.gov/documents/2025/08/22/2025-16139/personal-financial-data-rights-reconsideration.

Thank you for the opportunity to provide feedback to this RFI. We look forward to working with the House Financial Services Committee in continuing to assess federal consumer financial data privacy law.

American Bankers Association
America's Credit Unions
Bank Policy Institute
Consumer Bankers Association
Securities Industry and Financial Markets Association

Appendix A

American Bankers Association. The American Bankers Association is the voice of the nation's $25 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $19.7 trillion in deposits and extend $13.1 trillion in loans.

America's Credit Unions. America's Credit Unions is the unified voice for not-for-profit credit unions and their more than 144 million members nationwide. America's Credit Unions provides strong advocacy, resources and services to protect, empower and advance credit unions and the people and communities they serve. For more information about America's Credit Unions, visit AmericasCreditUnions.org.

Bank Policy Institute. The Bank Policy Institute ("BPI") is a nonpartisan group representing the nation's leading banks. BPI members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, BPI members hold $10.7 trillion in deposits in the United States; make 68% of all loans, including trillions of dollars in funding for small businesses and household mortgages, credit cards, and auto loans; employ nearly two million Americans and serve as a principal engine for the nation's financial innovation and economic growth.

Consumer Bankers Association. The Consumer Bankers Association represents America's leading retail banks. We promote policies to create a stronger industry and economy. Established in 1919, CBA's corporate member institutions account for 1.7 million jobs in America, extend roughly $4 trillion in consumer loans, and provide $275 billion in small business loans annually. Follow us on X @consumerbankers.

Securities Industry and Financial Markets Association. The **Securities Industry and Financial Markets Association ("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 one million employees, we advocate on 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. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA").

Appendix B

In preparing this document, the Associations met with their members to gather information on the challenges stemming from the patchwork of state privacy laws. Please see below for their aggregated feedback.

State privacy law frameworks can create duplicative requirements without corresponding benefit to consumer privacy. As one example, the recently finalized regulations implementing the CCPA impose fairly prescriptive requirements for an annual cybersecurity audit. As required under their GLBA and safety & soundness obligations, financial institutions already conduct extensive cybersecurity audits each year under other industry frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The California requirements risk forcing financial institutions to begin compiling a single annual cybersecurity audit for purposes of safely satisfying certain idiosyncratic California preferences, which will be duplicative of the numerous cybersecurity audits currently conducted by financial institutions that meet industry and prudential regulator standards.

Many members report fees for outside counsel and consultants to build compliance programs, which can run more than six figures. They must also engage technology and design departments to provide the necessary online disclosures. These disclosures can be confusing to consumers, particularly the "request to know" and "request to delete" rights. Deletion is especially challenging given the number of exceptions and abundance of retention laws for financial institutions. Moreover, many smaller institutions have to rely on vendor solutions, which are geared towards the European Union's General Data Protection Regulation and CCPA. These are not built with the financial sector in mind and are accordingly clunky.

Our members spent considerable time and resources building data access/deletion workflows and training staff. However, the number of requests is quite low (but could scale at any time). The population of substantive responses falling outside the GLBA exception is even smaller.

In addition, many of our members disable certain marketing features for states like California due to the potential for compliance risk. It also creates an environment that is onerous for startups and new companies, which might choose to withdraw from certain markets or not expand into them in the first place.

Further, app stores such as those maintained by Apple and Google often require certification with certain processes pursuant to state laws but are not tailored to reflect the nuances of the GLBA exemptions. Our members must adhere to these requirements or run the risk of their mobile apps being delisted. This introduces yet another hurdle for each new state law that is enacted.