August 28, 2025

By Electronic Submission to fsc119@mail.house.gov

The Honorable French Hill
Chairman, House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Andy Barr
Chairman, Subcommittee on Financial Institutions
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Re: Questions on Title V, Subtitle A of the Gramm-Leach-Bliley Act (GLBA)

Dear Chairmen Hill and Barr:

The Receivables Management Association International (RMAI) submits the following comments in response to your request for feedback on current federal consumer financial data privacy law and potential legislative proposals to account for changes in the consumer financial services sector.

I. INTRODUCTION

RMAI is a nonprofit trade association that represents over 600 companies that purchase or support the purchase of performing and nonperforming receivables on the secondary market. RMAI member companies include banks, credit unions, non-bank lenders, debt buying companies, collection agencies, law firms, brokers, and industry-related product and service providers. RMAI's Receivables Management Certification Program (also referred to as RMCP or Certification Program)[1] and its Code of Ethics[2] set the "gold standard" within the receivables management industry due to RMAI's rigorous uniform industry standards of best practice which focus on protecting consumers. Several of our standards have been adopted at the state level and

[1] Receivables Management Association International, *Receivables Management Certification Program, Ver. 10* (Mar. 1, 2023), publicly available at https://perma.cc/7D8Q-KGVC.
[2] Receivables Management Association International, *Code of Ethics* (August 13, 2015), publicly available at https://perma.cc/BM6J-USG.

were recently used as framework by the Uniform Law Commission in their Uniform Consumer Debt Default Judgment Act.[3]

Rolled out in 2013, RMAI's Certification Program sets high and robust industry standards that seek to go above and beyond the requirements of state and federal law for the protection of consumers.[4] While the program was first designed to certify debt buying companies, it has expanded to include certifications for law firms, collection agencies, and vendors (e.g., brokers and process servers). Currently, over 500 businesses and individuals hold these internationally respected certifications. Additionally, all the largest debt buying companies in the United States are RMAI certified, and we estimate that approximately 80 to 90 percent of all charged-off receivables that have been sold on the secondary market are owned by an RMAI certified company.

RMCP-certified businesses are subject to vigorous and recurring independent, third-party audits to demonstrate their compliance with the Certification Program. This audit includes an onsite inspection of the certified companies to validate full integration of RMCP standards into their business operations. Following a company's initial pre-certification audit and first full-compliance audit, independent program review audits continue to be conducted every three years. The audits are reviewed by an Audit Committee which has consumer representation. Since March 1, 2024, BBB National Programs has administered RMAI's Remediation Committee which is the committee that handles unresolved audit deficiencies.

RMCP certification also requires RMAI-certified businesses to engage a chief compliance officer, with a direct or indirect reporting line to the president, chief executive officer, board of directors, or general counsel of the business. The chief compliance officer must maintain individual certification through the RMCP by completing 24 credit hours of continuing education every two years.

Our members are subject to an extraordinary federal consumer financial services regulatory framework. Many of our members are covered "debt collectors" under the federal Fair Debt Collections Practices Act (FDCPA) (15 U.S.C. § 1692, *et seq.*). They are "furnishers" under the federal Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 *et seq.*) and "financial institutions" under the Gramm-Leach-Bliley Act (GLBA) (15 U.S. Code § 6801, *et seq*,). In addition, many of our members are supervised by the federal Consumer Financial Protection Bureau (CFPB) as "larger participants" or otherwise subject to CFPB enforcement.

---

[3] Uniform Consumer Debt Default Judgment Act, Prefatory Note ("this act seeks to incorporate provisions from . . . . standards set by Receivables Management Association International, a debt collections trade organization.") archived at https://perma.cc/T5TZ-CRC5.

[4] RMCP's Mission Statement reads in part, the certification program "is an industry self-regulatory program administered by RMAI that is designed to provide enhanced consumer protections through rigorous and uniform industry standards of best practice."

Among the federal regulations our members adhere to is the Safeguards Rule, 16 C.F.R. 314, *et seq*. The Safeguards Rule, promulgated under the GLBA by the Federal Trade Commission in 1999, requires financial institutions to create, implement, and maintain a comprehensive information security program to protect customer data.

States have recently adopted their own comprehensive consumer data privacy/data security laws. As we write this letter, 20 states have adopted comprehensive consumer data privacy laws, most having been adopted in the past three years. Unlike the federal Safeguards Rule, none of the state laws are fashioned for the consumer financial services industry. Instead, they apply to a wide variety of commercial enterprises. As a result, we have observed that several of these state laws require "one-size-fits-all" consumer disclosures that our members must deliver along with existing federal consumer disclosures designed for consumer financial services. These added generic disclosures are causing consumer confusion. Confusing consumers with inconsistent and often contradictory disclosures causes consumer harm. We outline these below.

We recommend the expansion of the GLBA to protect consumers from the confusing, inconsistent and often contradictory disclosures required by state laws Given the strong protections already afforded to consumers under the GLBA and the other federal privacy laws outlined above, there is little corresponding benefit to requiring financial firms to comply with a myriad of technical and often conflicting obligations. There does not appear to be any compelling position that protections under the GLBA are insufficient or are leading to any particular consumer detriment.

II. RESPONSES TO QUESTIONS

1. Should we amend the Gramm-Leach-Bliley Act (GLBA) or consider a broader approach?

We support the expansion of the GLBA to cover the use of Artificial Intelligence (AI) by financial institutions and in doing so preempt state AI laws affecting the provision of consumer financial services.

In 2025, the states introduced 1,294 bills concerning AI. While most of those bills do not impact financial institutions covered by the GLBA, we have identified 124 bills that would impact GLBA covered entities. Of those, most would cover the use of AI for automated decision making. Colorado, Maine, Texas, and Utah have enacted laws relating to the use of AI in many industries including "financial services."

State legislation is focused on the mere use of AI, and not whether the outcome from that use causes harm. In taking this odd approach, state legislation either conflicts, contradicts or

confuses the requirements imposed upon financial institutions by federal consumer financial services law to prevent the very harm these bills seek to redress.[5] [6] [7]

For example, debt collectors are required by 15 U.S.C. § 1692g of the FDCPA to provide certain disclosures to consumers within five days of their initial communication. One purpose of the § 1692g disclosure is to ensure the recipient is the true debtor and prevent dunning the wrong person.[8] The recipient can dispute owing the debt and even cause the debt collector to cease collection efforts. In doing so, the FDCPA provides a mechanism to prevent a covered debt collector from providing non-public personal information to people who mistakenly receive collection communication. These privacy protections have been in place since the FDCPA's adoption in 1978.

A California bill, A.B. 1018, would undo these protections. It would require a debt collector who uses an automated decision-making tool to disclose non-public personal information *before* verifying the debtor's identity under the FDCPA's 1692g mechanism. Such information debt collectors would be required to disclose could include social security numbers and credit histories. Worse, A.B. 1018 would also allow a recipient of a misdirected letter to "[c]orrect any incorrect personal information used by the covered [system] to make or facilitate the consequential decision." Because A.B. 1018 has no safeguards to verify the identity of the letter recipient, it opens the door for people who mistakenly receive a debt collection letter to corrupt the true consumer's personal and private financial data.

Unlike the state AI legislation, the federal framework regulating consumer financial services law is well positioned to adopt AI regulation that does not conflict with existing law and avoid the consumer harms state legislation like A.B. 1018 would create. Therefore, we support expanding the GLBA to cover the use of AI by financial institutions and in doing so preempt state laws affecting the provision of consumer financial services.

Any expansion of the GLBA to cover AI should be risk based, proportionate, designed to support innovation and competition, and potentially includes safe harbor provisions for GLBA entities using AI in accordance with any adopted federal standard.

---

[5] https://www.ftc.gov/legal-library/browse/rules/safeguards-rule

[6] https://www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fair-lending/index-fair-lending.html, archived at https://perma.cc/BM75-WGXV

[7] https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/, archived at https://perma.cc/CQ47-KNNN

[8] *Swanson v. S. Or. Credit Serv*., 869 F.2d 1222, 1225 (9th Cir. 1988) ("Congress designed the Federal Act to **'eliminate the recurring problem of debt collectors dunning the wrong person or attempting to collect debts which the consumer has already paid.'** S. Rep. No. 382, 95th Cong. 2d Sess. 4, reprinted in 1977 U.S. Code Cong. & Admin. News 1695, 1699. It added the validation of debts provision specifically to ensure that debt collectors gave consumers adequate information concerning their legal rights. *See id*. at 1702.") (emphasis added).

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

In addition to preempting state AI laws, a federal GLBA standard should preempt state privacy laws, especially to the extent they do not include entity-level exemptions for GLBA financial institutions, as discussed in more detail below.

Further, a preemptive standard is necessary to eliminate the confusion and costly compliance burdens incurred by GLBA financial institutions due to the growing patchwork of dissimilar state consumer data privacy laws.

We have observed that many states were simply unaware of existing federal consumer financial services privacy laws, like the FDCPA, FCRA, the GLBA and its Safeguards Regulation. It is noteworthy that numerous state data privacy bills introduced in the past several years did not include entity-level *or* data-level exemptions for GLBA financial institutions. In fact, some of those bills proposed data privacy regimes incomparable to any existing state law. Massachusetts H.1754 (2005), for example, is virtually a cut-and-paste version of the European Union's General Data Protection Regulation and would have a disproportionate negative effect on small and medium businesses.

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?

If the GLBA is made a preemptive federal standard, which RMAI supports, it should preempt state laws at least to the extent they lack entity-level exemptions for GLBA financial institutions.

When states exempt GLBA data but not GLBA financial institutions, it confuses consumers and presents practical compliance questions and excessive burdens for businesses. In such states, guesswork must be employed to determine which provisions of the laws apply if a non-exempt GLBA financial institution collects and processes *only* exempt GLBA data, which is common.

For example, financial institutions that collect *only* GLBA data provide state privacy notices that inform consumers of their privacy rights. However, when consumers seek to exercise those state law privacy rights, their requests are denied because all the financial institutions' data is subject to the GLBA exemption.

This scenario:

- confuses and aggravates consumers who received notice of their privacy rights, only to have them legitimately denied; and

- requires financial institutions to develop costly compliance procedures and employee training to receive and respond to consumer requests knowing the effort is meaningless since the GLBA data is exempt.

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

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

As with the state data privacy laws, which are general in nature, GLBA financial institutions and GLBA data should be exempt from any federal general data privacy law.

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

"Nonpublic personal information" is currently defined in the context of privacy regulations in the GLBA Privacy Rule.[9] The current definition is well established and understood in the financial services sector and does not require modification.

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

The definition of "personally identifiable financial information" in the GLBA Privacy Rule[10] is well established and understood in the financial services sector and does not require modification.

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

The definitions of "consumer" and "customer relationship" in the GLBA do not require modification.

The definitions of "consumer" and "customer relationship" are, by statute,[11] defined in the GLBA Privacy Rule.[12] These definitions and the examples are also included in the GLBA Safeguards Rule[13] and are well established and understood in the financial services sector.

[9] 16 C.F.R. § 313.2(n).
[10] 16 C.F.R. § 313.2(o).
[11] 15 U.S.C. § 6809(9) and (11), respectively.
[12] 16 C.F.R. § 313.3(e) and (i), respectively.
[13] 16 C.F.R. § 314.2(b) and (e), respectively.

The distinction between "consumer" and "customer," based on the "customer relationship," is an important one because it defines rights and responsibilities based on the nature of interaction.

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

   RMAI has no comment.

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

   With respect to GLBA financial institutions, the fifteen states that include entity-level GLBA exemptions[14] are effective privacy frameworks.

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

      RMAI has no comment.

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

   Consent should not be required before collecting certain types of data from, for example, service providers. Many GLBA financial institutions use service providers to obtain consumer data that is required to fulfill consumers' requests for products or services. IP addresses are also used to authenticate consumers and prevent fraud. Consumer consent is implied in those situations.

   In other situations, obtaining consumer data from service providers is necessary to enforce consumers' obligations, such as when they fail to make payments on a loan and collection or legal action becomes necessary. In that scenario, asking a consumer for consent to obtain information will almost always be futile.

   Additionally, PIN Numbers and IP addresses can be "personally identifiable financial information" under the GLBA privacy rule, which includes any information: "(i) A consumer provides to you to obtain a financial product or service from you; (ii) About a consumer resulting from any transaction involving a financial product or service between you and a

[14] Of the nineteen states that have enacted consumer data privacy laws, only California, Connecticut, Montana, and Oregon lack the entity-level exemption for GLBA financial institutions.

consumer; or (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer."[15]

Examples include:

- Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
- Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
- Any information you collect through an Internet "cookie" (an information collecting device from a web server).[16]

As such, PIN Numbers and IP addresses can be subject to the GLBA and exempt from the state consumer data privacy laws, and should not be made subject to a stricter federal standard.

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?

RMAI opposes 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.

First, it is unlikely a definition for "inactive" can be developed that will adequately address all types of accounts held by the variety financial institutions that differ in size, scope, product offerings, and services.

Second, data may be necessary more than one year after an account becomes inactive, depending on how "inactive" is defined, to enforce a consumer's obligation through collection activities or legal remedies.

RMAI recommends that any disposal requirement mirror, or be consistent with, the GLBA Safeguards Rule, 16 C.F.R. § 314.4(c)(6)(i):

> Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or

[15] 16 C.F.R. § 313.3(o)(1).
[16] 16 C.F.R. § 313.3(o)(2)(i)(D), (E), (F).

> regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

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

RMAI opposes a requirement requiring consumers to be provided with a list of entities receiving their data.

Even for the same type of product or service, a financial entity may use completely different service providers from one consumer to the next. Attempting to provide a list of each service provider that received each individual consumer's data will be prohibitively burdensome for businesses. It will also confuse consumers who, in most cases, will not recognize the names of the service providers or benefit from the knowledge.

Further, of the nineteen states that have enacted consumer data privacy laws, only one state has an unqualified right to request a list of specific third parties.[17]

RMAI suggests the current GLBA Privacy Rule requirement is sufficient, i.e., "[t]he categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information," subject to certain exclusions.[18]

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?

RMAI believes a financial institution should not be held liable if data it collects or holds is shared with a third-party, and that third party is breached, provided the financial institution has complied with the GLBA Safeguards Rule.

As to third parties, the GLBA requires financial institutions to oversee service providers, by:

> (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
> (2) Requiring your service providers by contract to implement and maintain such safeguards; and

---

[17] Only Minnesota provides consumers an unqualified "right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data." Minn. Stat. Ann. § 325M.14(h). In Connecticut, the right applies only if the consumer's personal data has been *sold*, Conn. Gen. Stat. § 42-518(a)(7) (effective July 1, 2026), and in Oregon a controller may, *at their option*, provide a list of specific third parties with whom personal data was shared, Or. Rev. Stat. Ann. § 646A.574(1)(a)(B).

[18] 16 C.F.R. § 313.6(a)(3).

(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.[19]

Further, no law should impose a strict liability standard upon a GLBA financial institution. Instead, a GLBA financial institution should be entitled to a bona fide error defense, e.g., it cannot be held liable if it shows by a preponderance of evidence that the violation was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adopted to avoid any such error.[20]

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?

Data minimization is a cornerstone principle of data privacy, but collection cannot be limited to only that needed to effectuate a consumer transaction because consumer financial data is also necessary to enforce consumers' financial obligations after effectuation of the transaction.

As discussed above, RMAI supports a disposal requirement that mirrors, or is consistent with, the GLBA Safeguards Rule, 16 C.F.R. § 314.4(c)(6)(i).

III. CONCLUSION

Based on the foregoing analysis, RMAI supports expansion of the GLBA to cover AI and to preempt state privacy laws and AI laws that seek to regulate entities covered by the GLBA. RMAI appreciates the opportunity to submit its comments concerning your questions. RMAI looks forward to assisting you in any capacity we can. Please do not hesitate to contact me if you need further clarification on RMAI's comments or if we can be of further assistance.

Sincerely,

Michael Becker

Michael Becker
Executive Director
Receivables Management Association International

[19] 16 C.F.R. § 314.4(f).
[20] See, for example, 15 U.S.C. § 1692k(c)

cc: RMAI Board of Directors