August 28, 2025

The Honorable French Hill
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Andy Barr
Chairman
Subcommittee on Financial Institutions
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

RE: Community Bank Perspective on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals

Dear Chairmen Hill and Barr:

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to provide comments on the request for feedback on current federal consumer financial data privacy law and potential legislative proposals. As the only national trade association dedicated exclusively to serving the interests of community banks, ICBA represents nearly 50,000 community bank locations of varying asset sizes across the United States.

Since its enactment in 1999, the Gramm-Leach-Bliley Act (GLBA) has served as the cornerstone of consumer financial privacy law. For community banks, GLBA has provided a well-established framework for safeguarding sensitive customer information, ensuring transparency through privacy notices, and implementing strong safeguards for data security. Over the past two decades, community banks have invested heavily in compliance systems, staff training, and customer education to meet GLBA's requirements, despite operating with fewer resources than larger institutions. While the law has been effective in establishing a trusted baseline, the emergence of new technologies, data aggregators, and fintech partnerships has created both gaps and inefficiencies in the current system.

Summary Recommendations

- ICBA believes that targeted amendments to the Gramm-Leach-Bliley Act (GLBA) are the most appropriate course of action, rather than pursuing a broader or wholesale replacement of the law.
- GLBA amendments must update and clarify definitions to address modern data practices such as the growing role of data aggregators and third-party technology providers. Non-banks obligations under GLBA should be subject to equivalent to bank obligations.
- ICBA supports adoption of a preemptive federal GLBA standard to establish a strong and consistent

[1] *The Independent Community Bankers of America ® has one mission: the create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovation offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit ICBA's website at icba.org.*

- baseline applicable to all entities handling consumer financial data, while eliminating the unnecessary compliance fragmentation.
- ICBA encourages the committee to ensure that any preemptive federal GLBA standard provides clear and comprehensive preemption, resolving the uncertainty created by state privacy laws that rely solely on data-level exemptions. A modernized GLBA should apply at the entity level rather than the data level.
- GLBA should serve as the exclusive standard for financial institutions and should apply at the entity level while being harmonized with general federal privacy legislation to promote consistency across industries.

See ICBA's detailed responses below to the committee's questions. We expand on the above-stated principles and provide a more technical discussion. We welcome the opportunity to discuss these recommendations in greater detail and to serve as a resource on the unique operational realities of community banks.

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

ICBA cautions against adopting a broader approach that could result in duplicative or conflicting regulatory regimes. ICBA believes that targeted amendments to the Gramm-Leach-Bliley Act (GLBA) are the most appropriate course of action, rather than pursuing a broader or wholesale replacement. Community banks are already among the most heavily regulated financial institutions and have invested significant resources in developing compliance programs under the GLBA framework. Frequent or wholesale changes would impose disproportionate burdens on smaller institutions while creating regulatory uncertainty for the sector.

The primary regulatory gap is oversight of non-bank entities handling consumer financial data. Targeted amendments should focus on clarifying definitions and ensuring the statute keeps pace with modern data practices. In particular, the committee should clarify terms such as "non-public personal information," "financial institution," and "customer relationship" to better account for the evolving digital landscape and the growing role of data aggregators and third-party technology providers. Importantly, these non-bank entities should be subject to equivalent obligations under GLBA to ensure consistency and fairness in consumer financial data protection.

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

ICBA urges the committee to use preemption to establish a strong and consistent baseline applicable to all entities handling consumer financial data, while eliminating unnecessary compliance fragmentation. Community banks are deeply committed to safeguarding consumer financial data, but the current federal approach creates a compliance landscape that is increasingly fragmented. States are adopting divergent privacy laws with varying definitions, notice requirements, and enforcement provisions. For community banks that operate across state lines, this results in duplicative compliance costs, operational complexity, and heightened legal risk. At the same time, preemption must not weaken consumer confidence by lowering protections.

Question 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?

ICBA encourages the committee to ensure that any preemptive federal GLBA standard provides clear and comprehensive preemption, resolving the uncertainty created by state privacy laws that rely solely on data-level exemptions.

Several states—including California, Connecticut, Minnesota, Montana, and Oregon—currently exempt only "nonpublic personal information" regulated under GLBA, rather than providing an entity-level exemption, leaving financial institutions subject to overlapping state privacy requirements for other categories of data.

To address this challenge, ICBA recommends that a federal GLBA standard:

1. Apply at the entity level rather than the data level, ensuring that GLBA-regulated financial institutions are comprehensively governed by a single, uniform framework.
2. Make clear that GLBA compliance constitutes the exclusive privacy and data security obligation for covered financial institutions, eliminating duplicative or conflicting state requirements.
3. Extend consistent obligations to non-bank entities, including data aggregators and fintech providers, to close existing regulatory gaps and prevent arbitrage.

Absent clear preemption, state-level data exemptions will continue to impose unnecessary and costly burdens on community banks while doing little to enhance consumer protections.

Question 4: How should GLBA relate to other federal consumer data privacy laws, both a potential general data privacy law and current sector-specific laws? Should GLBA "financial institutions" be subject to entity-level or data-level exemptions from these laws?

ICBA recommends that GLBA remain the primary and comprehensive framework for financial institutions, with its obligations harmonized against any future general federal privacy law and existing sector-specific statutes. This approach will provide consumers with strong, uniform protections, while enabling community banks to maintain compliance without unnecessary duplication or disproportionate burden.

Community banks already comply with robust federal standards under GLBA, along with complementary frameworks such as the Bank Secrecy Act (BSA), Fair Credit Reporting Act (FCRA), and the Right to Financial Privacy Act. Layering additional compliance obligations from a general consumer privacy law on top of GLBA would create duplication, increase costs, and heighten regulatory uncertainty—especially for smaller banks that lack the compliance infrastructure of larger institutions.

To ensure clarity, ICBA supports an entity-level exemption for financial institutions subject to GLBA from general data privacy laws. This approach would make compliance with GLBA sufficient for all categories of data handled by regulated institutions, eliminating the risk of parallel or conflicting obligations based on data classifications. At the same time, the committee should ensure that non-bank entities such as data aggregators and fintech providers are held to comparable standards, closing regulatory gaps and preventing arbitrage.

Question 5: How should we define "non-public personal information" within the context of privacy regulations? Does the term "personally identifiable financial information" in GLBA require modification?

ICBA recommends retaining the current structure of GLBA's definition of "nonpublic personal information" (NPI) and "personally identifiable financial information," while modestly updating the framework to reflect today's digital environment. Community banks have long relied on these definitions to build effective compliance programs, and they are well understood by regulators, institutions, and consumers. Wholesale redefinition could undermine this stability and impose unnecessary costs on smaller institutions without providing meaningful additional consumer protection.

At the same time, the committee should modernize GLBA definitions to account for the types of information increasingly used in the financial ecosystem. This includes digital identifiers (such as IP addresses and device identifiers), biometric information used in authentication, and derived financial profiles created through algorithms and analytics. Explicitly recognizing these categories within the definition of NPI would provide greater clarity and ensure consistent protections.

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

ICBA recommends retaining the current structure of the definitions of "consumer" and "customer relationship" in GLBA, while providing targeted clarifications to reflect modern banking practices and digital engagement. To provide a more consistent approach, Congress should amend the definition of a "consumer" in Section 1033 of the Dodd Frank Act to match the definition in GLBA.

The existing definitions have provided a workable and consistent framework for more than two decades. Community banks, regulators, and consumers all understand these terms, and wholesale changes would risk introducing confusion and costly compliance disruption, particularly for smaller institutions.

To reflect the realities of today's digital banking environment, the definitions should confirm that:

1. Consumers include individuals engaging with financial institutions through online and mobile platforms, not solely through in-person interactions.
2. Customer relationships may be established electronically, including when consumers provide information through digital applications, online account openings, or mobile enrollment processes.
3. Clarification is needed on how third-party intermediaries, such as fintechs and data aggregators, affect the establishment of a customer relationship, and whether end-users interacting with a bank through such channels should be deemed customers of the bank, the intermediary, or both.

Maintaining the current framework while modernizing it for digital interactions will provide clarity and prevent gaps in accountability—without imposing unnecessary compliance burdens on community banks.

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

ICBA believes the current definition of "financial institution" under GLBA should be expanded to more clearly capture non-bank entities that collect, aggregate, or process consumer financial data, including data aggregators, fintech firms, and technology providers.

Many non-bank actors that handle equivalent or greater volumes of consumer financial information than banks operate outside the GLBA framework. This regulatory disparity creates significant risks:

- Consumer Protection Gaps. Consumers often cannot distinguish between regulated banks and unregulated third parties that handle their financial data. When aggregators or fintechs experience a breach, consumers' trust in the broader financial system is undermined;
- Regulatory Arbitrage. Non-bank entities can exploit lighter obligations, gaining competitive advantage over community banks that already shoulder disproportionate compliance costs; and
- Third-Party Risk Transfer. Community banks are increasingly required to partner with fintechs and third-party providers to deliver digital services. Without clear accountability under GLBA, banks are left to manage risks that should be borne directly by these providers.

To close these gaps, ICBA recommends the committee explicitly include data aggregators, fintechs, and other entities that collect or process consumer financial information within the scope of GLBA Title V.

Question 8: Are there states that have developed effective privacy frameworks? Which specific elements from these state-level frameworks could potentially be adapted for federal implementation?

ICBA encourages the committee to incorporate the entity-level exemption principle into any modernization of GLBA or broader federal privacy framework. This approach would ensure the GLBA remains the exclusive standard for financial institutions, delivering the clarity and uniformity that consumers, regulators, and community banks need while eliminating the costly patchwork of conflicting state laws.

Several states have enacted comprehensive privacy laws, but most rely on data-level exemptions for financial information, which creates compliance uncertainty for community banks. ICBA urges the committee to view the Kentucky and Indiana models as examples of how entity-level exemptions can provide both clarity for institutions and consistent protections for consumers. These states have developed the most effective privacy frameworks by adopting entity-level exemptions for GLBA-regulated institutions.

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

Requiring prior consumer consent for the use of such technical information could hamper fraud prevention, introduce unnecessary friction into digital banking services, and ultimately place consumers at greater risk. For these reasons, ICBA recommends the committee preserve flexibility for financial institutions to collect and use technical data elements necessary to fulfill their fraud prevention,

cybersecurity, and compliance obligations, while continuing to apply strict safeguards for highly sensitive information such as PINs and authentication credentials.

ICBA agrees that certain categories of highly sensitive data—such as PIN numbers, biometric identifiers, and authentication credentials—should only be collected and used with strong security protections in place. These data elements are directly tied to account access and financial security, and misuse could expose consumers to significant fraud and identity theft risks.

However, ICBA cautions against imposing blanket consent requirements for routine data elements such as IP addresses, geolocation data, or device identifiers. For community banks, the collection of this information is critical for fraud detection, cybersecurity monitoring, and regulatory compliance. For example:

- Fraud Monitoring. IP addresses and device data allow institutions to detect suspicious activity, such as account takeover attempts, by flagging logins from unusual locations or devices;
- Cybersecurity Defense. Technical identifiers are essential for monitoring and blocking malicious traffic, protecting both consumers and the financial system as a whole; and
- Regulatory Compliance. Federal guidance and supervisory expectations (including those from the Federal Financial Institutions Examination Council (FFIEC) and prudential regulators) require banks to implement robust systems for customer authentication, fraud detection, and cyber risk mitigation—systems that rely on these forms of data collection.

Question 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?

ICBA does not support a mandatory requirement for financial institutions to delete consumer data after one year of inactivity. While the intent of reducing unnecessary data retention is understandable, such a rule would conflict with long-standing federal and state regulatory and legal requirements for data retention and would expose community banks to heightened operational and compliance risk.

Community banks are already subject to a broad range of recordkeeping obligations under laws such as the Bank Secrecy Act (BSA), anti-money laundering (AML) regulations, tax reporting requirements, and prudential supervision standards. These laws require financial institutions to maintain customer records for multiple years—commonly five to seven years—to support regulatory examinations, fraud investigations, litigation defense, and law enforcement inquiries. A rigid one-year deletion mandate would directly conflict with these obligations and create significant legal exposure for community banks.

Additionally, customer data associated with inactive accounts often plays a critical role in fraud prevention, cybersecurity monitoring, and identity verification. Historical data can be used to confirm account ownership, detect suspicious activity, and protect against account takeover schemes.

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

ICBA supports transparency in data sharing but cautions against imposing rigid requirements that would mandate providing consumers with detailed lists of every third party receiving their information. Community banks already provide clear and standardized privacy notices under GLBA's privacy rule,

which require disclosure of the categories of information collected, the categories of third parties with whom it is shared, and the purposes for such sharing. These notices strike an appropriate balance between consumer transparency and operational feasibility.

Mandating that institutions provide a continuously updated, entity-by-entity list of all recipients would introduce several risks and challenges:

- Operational Burden. Community banks rely on numerous vendors, service providers, and regulators. Maintaining real-time, entity-specific lists would create significant administrative challenges and expose institutions to liability for inadvertent errors;
- Consumer Confusion. A long list of named entities may overwhelm or confuse consumers, offering little practical value compared to clear disclosure of categories and purposes; and
- Cybersecurity Risk. Publicly disclosing specific vendor and partner lists could inadvertently create a roadmap for malicious actors. If these lists were to fall into the wrong hands, they could expose community banks' vendors and service providers to targeted fraud, phishing, and cyberattacks.

Any expanded disclosure requirements should also apply to non-bank data aggregators and fintech providers, which currently operate outside of the GLBA framework yet handle large volumes of consumer financial data.

Question 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?

Community banks face extensive supervisory expectations for vendor management and third-party risk oversight, including requirements to conduct due diligence, negotiate contractual protections, and monitor ongoing compliance. These obligations, enforced by federal banking regulators through the FFIEC Interagency Guidance on Third-Party Relationships, ensure that banks take appropriate steps to mitigate vendor risks.

However, in light of the planned implementation of Section 1033 of the Dodd-Frank Act, we believe that Congress should create a liability framework that indemnifies community banks for breaches that occur at third-party data recipients when the customer has authorized data sharing with the third-party. Community banks do not have control over which third parties their customers share data with, nor do they have control over the steps to protect customer data taken by those third parties. In addition, third parties and aggregators may share customer data with other third parties that the community bank acting as a data provider is not even aware of.

Open banking may require community banks to share data with third parties they do not have an existing contractual relationship with and who they have not had a chance to thoroughly vet. It would be unreasonable to hold banks liable for breaches at these third parties. At a minimum, Congress should create clearer rules surrounding when a bank is permitted to refuse a third-party request for customer data – even if authorized by the customer – when the bank has not been able to verify the third party's compliance with the data protections required by the GLBA.

To ensure that customer data remains protected in the world of open banking, Congress should also require the Consumer Financial Protection Bureau to supervise non-bank financial institutions that act as data recipients for compliance with the GLBA.

Question 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?

Community banks have a long tradition of building relationships based on trust, and responsible data stewardship is central to maintaining that trust. ICBA supports the principle of data minimization and agrees that financial institutions should collect and retain only the information necessary to provide financial products and services, protect consumers from fraud, and comply with legal and regulatory obligations.

ICBA cautions that rigid or prescriptive data minimization and retention rules could conflict with existing federal requirements and supervisory expectations. As previously mentioned, financial institutions are subject to extensive recordkeeping obligations under varies laws and regulations. Imposing blanket federal limits that shorten these periods could place community banks in direct conflict with their legal obligations.

Additionally, historical consumer data plays a critical role in fraud detection, identity verification, and risk management. Community banks use past data patterns to identify unusual transactions, prevent account takeovers, and respond to law enforcement inquiries. Overly restrictive retention rules could undermine these essential protections and expose consumers to greater risk.

ICBA recommends the committee encourage flexible, risk-based data minimization standards that recognize the unique compliance environment of financial institutions. This approach will strengthen security and promote responsible data practices without placing community banks in the untenable position of choosing between compliance with GLBA and other laws.

In closing, ICBA looks forward to working with the committee to modernize GLBA in a way that maintains strong consumer protections, provides uniform and predictable national standards, and ensures proportional, scalable compliance for community banks while extending comparable obligations to non-bank data handlers.

Sincerely,
/s/
Rebeca Romero Rainey
President & CEO