America's Credit Unions

Testimony of

Andrew Morris
Director, Innovation and Technology
America's Credit Unions

Hearing: "Framework for the Future: Reviewing Data Privacy in Today's Financial System"

Before the
Subcommittee on Financial Institutions
House Committee on Financial Services

June 5, 2025

Introduction

Good morning, Chairman Barr, Ranking Member Foster, and Members of the Subcommittee. I am Andrew Morris, Director of Innovation and Technology at America's Credit Unions. America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the credit union industry to effectively meet the needs of their over 142 million members nationwide. Thank you for the opportunity to testify about how a comprehensive federal privacy law can be harmonized with the existing laws and regulations applicable to credit unions.

First and foremost, America's Credit Unions supports a comprehensive federal data security and privacy framework that includes robust security standards that apply to all who collect or hold sensitive personal data. We recognize that the financial services landscape is evolving. It is important that as the law evolves to match it, credit unions have rules of the road that allow them to meet the needs of their members in the marketplace. This includes a data privacy standard that not only protects their members but also allows credit unions to evolve in their service to them.

As Congress considers changes to data privacy requirements, there are three key tenets that credit unions believe must be addressed in any new national data privacy law:

1. A recognition of Gramm-Leach-Bliley Act (GLBA) standards and accompanying regulations in place for financial institutions and a strong exemption from new burdensome requirements;
2. Robust federal preemption from a patchwork of state laws for credit unions in compliance with national privacy and GLBA standards; and
3. Protection from frivolous lawsuits created by a private right of action.

Existing Law on Data Privacy and Security

Depository institutions, including credit unions, have long been subject to a framework of laws and regulations designed to ensure a high standard of consumer privacy and data security. Central to this framework is Title V of the GLBA, which acknowledges the need

for heightened care when handling sensitive consumer financial information and provides well-established standards for addressing consumer privacy concerns. Other laws, such as the Fair Credit Reporting Act (FCRA) and Right to Financial Privacy Act (RFPA) have also operated to protect credit union member privacy for nearly 50 years.

America's Credit Unions believes that the GLBA should remain the model for depository institution compliance with any future federal data security and privacy standard.

The GLBA mandates specific disclosure of how nonpublic personal information is collected and shared by financial institutions. The Consumer Financial Protection Bureau's (CFPB) Regulation P implements the GLBA's privacy provisions. It requires disclosures of privacy policies, places limits on sharing certain information for marketing purposes, and gives consumers the right to opt out of certain types of information sharing with nonaffiliated third parties.[1] In addition to an initial privacy notice, credit union members receive an annual notice describing their credit union's privacy policy which outlines, among other things, the types of information sharing individual members can decline.

In general, federal law gives credit union members the right to decline sharing creditworthiness information for affiliates' everyday business purposes, the use of information by affiliates for marketing purposes, and the sharing of information with nonaffiliates for marketing purposes.[2] Under Regulation P, if a credit union changes its policies and practices regarding disclosures to nonaffiliated third parties so that its most recent notice is inaccurate, then the credit union may not begin disclosing the information until it provides revised privacy notices and opt-out procedures.[3]

Additionally, credit unions, like many financial institutions, have long prioritized investments in data security to ensure that their members' privacy is protected. The GLBA requires financial regulators to implement technical safeguards to ensure that financial

[1] *See* 12 CFR Part 1016.
[2] *See* Appendix to Part 1016 - Model Privacy Form.
[3] *See* 12 CFR 1016.8.

institutions are protecting their customers' information.[4] These safeguards are comprehensive and designed to ensure the (i) security, (ii) confidentiality, (iii) integrity, (iv) and proper disposal of consumer information and other records. Under the rules promulgated by the National Credit Union Administration (NCUA) for credit unions, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require credit unions to ensure that third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

The NCUA also demands regular risk assessments of data security programs, as well as mechanisms to address incidents of unauthorized access to sensitive member information. While the threat of incurring reputational injury already provides a significant incentive to guard member data closely, numerous legal obligations and volumes of regulatory guidance also operate to protect member data.

The NCUA's data security rules are supplemented by a large body of regulatory guidance developed by the Federal Financial Institutions Examination Council (FFIEC) that takes the form of booklets covering various information security topics. The FFIEC, which is comprised of various banking regulators, including the NCUA, has devoted hundreds of pages of guidance to the topics of IT security, architecture, infrastructure and operations, audits, and many other topics. For example, the FFIEC has advised its regulated financial institutions to "restrict and monitor data extraction" and limit the ability to view or modify data to only what is necessary to carry out job responsibilities and automated functions—principles of access control that help achieve the goal of data minimization.[5]

The FFIEC has also documented numerous security controls such as employing an appropriate level of encryption on data in transit and data at rest based on the type and criticality of the information. In the domain of data analytics, the FFIEC has advised regulated financial institutions to identify "processes to remove or destroy data when no

[4] *See* 12 CFR Part 748.
[5] *See* FFIEC, Architecture, Infrastructure and Operations, 18-19 (2021), *available at* https://ithandbook.ffiec.gov/media/ywfm2ftz/ffiec_itbooklet_aio.pdf.

longer used in the data analytics tools." Collectively, these principles and controls, along with many others too numerous to name, contribute to a robust data security environment that is designed to guard the privacy of credit union members' nonpublic personal information.

In addition to the large volume of regulatory guidance derived from the safeguards provisions of the GLBA, examination-based supervision provides another important layer of protection. Not all financial institutions, as defined under the GLBA, are subject to periodic examination by a functional regulator like the NCUA. That difference matters in terms of how a future federal privacy framework accounts for the rigor and scope of existing compliance. It is also a key reason why America's Credit Unions supports a clear entity-level exemption for credit unions subject to the GLBA.

Key Elements and Issues in Any Future Data Privacy Regime

As Congress considers potential reforms to data privacy and security, there are various aspects we believe should be included or addressed:

<u>An Entity Level Exemption is Appropriate for Depository Institutions</u>

In the context of a future federal privacy framework, an entity-level exemption would recognize the rigor of existing financial institution compliance activities and allow the prudential financial regulators and CFPB, as appropriate, to tailor supervision based on changing privacy or data security risks. An entity-level exemption for financial institutions, such as credit unions, would also address administrability concerns often associated with alternative frameworks that offer only a data-level exemption.

For context, the less preferred data-level exemption typically operates on the principle that specific types or uses of data addressed by other federal laws can be set aside as adequately regulated. However, a data-level exemption provides limited relief in practice. This is because the extent of relief is confined to narrow categories or uses of data which must be matched to federal statutory language.

Unfortunately, the GLBA and other federal privacy laws were written decades ago, and do not articulate in detail all the types of data or data processing activities relied upon by credit unions today. Supervisory guidance developed by the FFIEC and the NCUA supplement the GLBA, but the statutory language itself tends to focus on high level aspects of information exchange. As a consequence, even understanding the scope of a data-level exemption can be a complex undertaking because it requires a credit union to reconcile uniquely defined categories of data with federal laws, which may not afford great specificity. For example, this could require a credit union to grapple with uniquely defined categories of data and perform a top to bottom inventory of every data element being processed by the credit union or any of its affiliates. That consumes time and resources that could be better spent delivering affordable credit to Americans, particularly those in rural and underserved communities.

Recognizing these challenges, various state legislatures have adopted entity-level exemptions in their own privacy laws for financial institutions that comply with the GLBA. Some states have opted for a combination of data-level and entity-level exemptions for added flexibility.

The American Privacy Rights Act from the 118th Congress took the approach of recognizing an exemption for financial institutions but only to the extent of *compliance* with existing federal data privacy or data security laws and only "with respect to the activities governed by the requirements of such law or regulation."[6] While this arrangement would have potentially spared certain financial institutions from conflicting provisions related to affiliate data sharing, opt-out procedures, and delivery of disclosures, it would not have covered other uses of data. This left the door open for introducing new compliance procedures for data used in conjunction with artificial intelligence, or data portability standards and any other areas not specifically addressed by the GLBA.[7] Such a limited exemption would have done little to spare credit unions

[6] *See* e.g., Sec. 118(b)(3) of H.R.8818 - American Privacy Rights Act of 2024 [introduced].
[7] *See* e.g., Sec. 105 of H.R.8818 - American Privacy Rights Act of 2024.

from the additional compliance costs and burdens associated with analyzing data processing activities not specifically enumerated by the GLBA.

Delegation of Authority to Appropriate Sectoral Regulators

The oversight of credit unions, banks, and other depository institutions is best left to the functional financial institution regulators that have experience in this field. America's Credit Unions does not support an approach to federal privacy regulation which grants overlapping supervisory authority to a secondary agency that does not have direct experience examining credit unions.

For example, the NCUA is the sole regulator equipped with the requisite knowledge and expertise to regulate credit unions. The NCUA is well versed in the unique nature of credit unions and has served as the primary regulator for credit unions since its inception. As such, in the area of privacy enforcement, the NCUA should be the primary regulator of credit unions and collaborate with other regulators on joint rulemaking when necessary. With the appropriate regulatory authority, the NCUA can ensure credit unions maintain a safe and sustainable information system.

Preemption of State Laws is Necessary

For financial institutions already shouldering high compliance burdens associated with examination-based supervision, an entity-level exemption is just one essential component for any comprehensive federal privacy framework. Preemption of a conflicting patchwork of state laws is also needed.

Today's patchwork of state privacy laws has invited idiosyncratic approaches to data processing activities and technologies. Some states, by choosing to recognize only a data-level exemption, have placed strains on credit unions by demanding more complex procedures, such as performing a comprehensive inventory of all institution-held data, in order to comply with specific disclosure requirements. The resulting compliance burdens, magnified each time a new state law is passed, siphon resources away from service to consumers and the core lending activities of credit unions.

Some previous legislative proposals for comprehensive federal privacy legislation contemplated preemption of state laws, but the inclusion of numerous exceptions greatly eroded the intended relief. For example, preservation of state laws related to regulating deceptive, unfair, or unconscionable practices could have easily circumvented intended areas of preemption given that the analysis relied upon when identifying "unconscionable" practices tends to invite jurisdictional expansion—a phenomenon we have witnessed from regulators in the past.[8]

Federal preemption carveouts intended to accommodate state rules for reporting cyber incidents could also give rise to inconsistencies and perpetuate administrative compliance over actual response and recovery activities if an institution does suffer a cyber incident. Credit unions must already notify members "as soon as possible" under Part 748 of the NCUA's regulations if sensitive member information is accessed by an unauthorized party, and must notify the NCUA within 72 hours if the credit union or a third party handling credit union systems or data experiences a substantial cyber incident. Credit unions are also covered by the Cyber Incident Report for Critical Infrastructure Act and are likely to face additional implementing regulations promulgated by the Cybersecurity and Infrastructure Security Agency later this year.

The purpose of a comprehensive federal privacy standard is to synthesize the current patchwork data protection laws under a uniform national standard. Financial institutions must be able to effectively serve their members across jurisdictions and should not be exposed to the unnecessary compliance burdens of potentially 50 different privacy laws in 50 different states. Even though some existing federal privacy laws do not preempt state laws, there are numerous examples of preemption in existing federal privacy law. Currently, at least three federal privacy statutes have preemption provisions under which states may not regulate the specific area of law covered or enact laws that impose additional requirements or prohibitions. For example, the Children's Online Privacy Protection Act, the CAN-SPAM Act, and the FCRA all have some state preemption

[8] *See* e.g., American Privacy Rights Act.

provision.[9] The purpose of privacy and cybersecurity laws is only achievable if the protections put in place are both comprehensive and consistent. Without consistent privacy and data security requirements in place, bad actors will simply identify the jurisdictions with the weakest or no requirements and use organizations in those jurisdictions for entry into interconnected networks across the country.

Complexity of Data Deletion

Certain features of proposed privacy frameworks, such as prohibitions on collecting certain types of metadata without consumer opt-in, or a broad right of deletion, similar to what is found in the EU's General Data Protection Regulation (GDPR), can frustrate efforts to comply with recordkeeping rules, or to detect and prevent fraud.

Data deletion requirements are particularly challenging for credit unions and other financial institutions that are subject to various recordkeeping requirements. For example, Regulation E requires any person subject to the Electronic Fund Transfer Act (EFTA) to retain evidence of compliance with the EFTA's requirements for a period of not less than two years from the date disclosures are required to be made or action is required to be taken.[10]

Given that compliance with Regulation E practically demands retention of customer transaction data as well as other information that might bear upon the validity of a transaction (e.g., IP address, geolocation, device data, etc.), deletion of such information may frustrate a credit union's ability to demonstrate that it relied upon appropriate sources of data when investigating an allegedly unauthorized electronic fund transfer. However, the EFTA's provisions related to investigations of transactions or errors do not necessarily demand the collection of transactional metadata—those are practices adopted by practical necessity. The distinction is critical because states that have adopted data deletion rights sometimes condition exceptions to that right on the existence of a "legal obligation" or a specific type of security related activity.[11] The EFTA's error resolution and

[9] *See* 15 U.S.C. §§ 6501–6506; 15 U.S.C. §§ 7701-7713; 15 U.S.C. § 1681t(a).
[10] *See* 12 CFR 1005.13(b).
[11] *See e.g.*, California Consumer Privacy Act, Cal Civ. Code 1798.105(d).

investigation requirements, which influence the extent of financial institution liability, are retrospective analyses (meaning they do not prevent fraud in a direct sense) and do not obligate collection of data—so the application of such an exception would be unclear, at best.

Likewise, for credit unions, the NCUA's regulation implementing the Truth in Savings Act (TISA) provides that a credit union shall retain evidence of compliance for a minimum of two years after the date disclosures are required to be made or action is required to be taken. TISA's rules regarding consumer advertising may incentivize a credit union to retain technical information about how advertisements are deployed across digital channels, which may involve collection of device and IP address information from consumers. While there is no requirement in TISA that would obligate a credit union to collect or retain metadata about such interactions, it may be useful information to have for documenting compliance. While some privacy frameworks carve out data deletion exceptions for certain internal uses of data, undertaking the analysis to determine whether a particular use is "reasonably aligned with the expectations of the consumer" or "compatible with the context in which the consumer provided the information" can involve significant and repeated analysis. As noted previously, the rigor of existing examination-based supervision already ensures that the use of data complies with privacy and security safeguards established under the GLBA and Part 748 of the NCUA's regulations.

Broad data deletion rights can also greatly complicate the ability of financial institutions to deploy artificial intelligence (AI) which is trained on consumer transactional history, interactions, or other behavioral characteristics. The discrete events which may involve collection of consumer data will not always implicate an obvious security concern—for example, transcribing a routine customer service interaction—but the historical value of this data is important for retrospective analysis when developing tools to detect anomalous behavior and fraud. Because AI fraud models work best when they understand both normal and abnormal behavior, a patchwork of data deletion rights coupled with idiosyncratic exceptions could impair the usefulness of such technology. It may also be impractical for a credit union that has ingested certain types of training data within a fine-

tuned model to selectively delete information without having to incur the enormous expense of retraining the model from scratch using a new data set every time historical information is removed. Simply put, data deletion requirements done haphazardly could hinder efforts of financial institutions to protect consumers and fight fraud.

Opt-In vs. Opt-Out

The GLBA and Regulation P generally operate to limit sharing of sensitive consumer information through an opt-out process, something we believe should continue and be the standard for financial institutions in any future data privacy regime.

Safe Harbor

A comprehensive federal data privacy framework should provide for principles-based requirements and offer a safe harbor for businesses that take the appropriate steps to comply with the law.[12] For example, the guidelines in the NCUA's Part 748 require credit unions to develop and implement an information security program that includes board approval; oversight and reporting; the assessment, management, and control of appropriate risks surrounding the security of member information; and regular testing and appropriate adjustment of the program. This risk-based approach is appropriate because it requires organizations to assess their own risks and implement protections proportionate to those risks. A prescriptive requirement will necessarily result in a misalignment between the risk to the consumer and the organization and the protections put in place. In general, a financial institution subject to the GLBA that develops tailored privacy and data security processes and procedures based on an appropriate risk assessment should be found to be in compliance with the law.

Private Right of Action

Some state privacy laws and proposed federal privacy legislation have incorporated a private right of action which permits consumers to sue businesses if they fail to comply with specific rules related to safeguarding information. In general, consumers can already bring causes of action against businesses when they suffer injuries related to the

[12] See 15 U.S.C. § 7707(b)(1).

mishandling of data. Those causes of action have traditionally relied upon theories of negligence or breach of contract. A federal private right action would be distinguishable insofar as it could invite lawsuits more focused on compliance violations rather than evidence of actual injury or economic loss. A private right of action would also perpetuate gradual variances in judicial interpretations, undermining the purpose of preemption by establishing different tests for assessing injury or harm.

Some have critiqued the private right of action as inviting trial lawyers to extract lucrative settlements from businesses based on perceived lapses in compliance. It is not uncommon for financial institutions to agree to settlement, even if they have committed no wrong, simply due to the costs of protracted litigation and discovery involving the accounts of potentially millions of consumers. America's Credit Unions has serious concerns with any broad private right of action due to the risk of frivolous lawsuits being filed against credit unions which are already held accountable for compliance violations by their regulator, the NCUA, as well as the CFPB. Furthermore, it is unlikely that a private right of action would offer any meaningful enhancement to the enforcement jurisdiction of the NCUA, which already requires credit unions to report incidents involving unauthorized access to member information to both supervisory points of contact as well as affected members. Adding additional costs to credit unions, and ultimately their members, through contending with lawsuits under an expansive private right of action would do little to improve compliance with the law, while doing more to hinder their ability to provide services to their members.

Conclusion

Stringent information security and privacy practices have long been a part of the financial services industries' business practices and are necessary as financial services are entrusted with consumers' nonpublic personal information. Still, the financial marketplace is evolving. While not the subject of today's hearing, issues such as open banking and AI will interplay with privacy issues in the future. Protection of consumer financial information is an important tenet of the financial services industry. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the GLBA, RFPA, FCRA

and other federal laws and regulations. The GLBA's technical safeguards and privacy protections are strengthened by federal and state regulators' examinations, implementing regulations, and robust enforcement for violations of the GLBA's requirements.

Ultimately, America's Credit Unions believes that when considering a comprehensive future federal privacy framework, Congress should prioritize the following features:

- A recognition of GLBA standards and accompanying regulations in place for financial institutions through the adoption of an entity-level exemption;
- Strong federal preemption from the myriad of various state laws for those in compliance with federal privacy and GLBA standards; and
- Protection from frivolous lawsuits created by a private right of action

We look forward to working with you to achieve such a framework.

Thank you for holding this important hearing and the opportunity to appear before you today. I welcome any questions you may have.