



3138 10th Street North
Arlington, VA 22201-2149
703.842.2215 | 800.336.4644
f: 703.522.2734
dberger@nafcu.org | nafcu.org

B. Dan Berger
President & Chief Executive Officer

National Association of Federally-Insured Credit Unions

January 23, 2020

The Honorable Kathleen Kraninger
Director
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

RE: Data Privacy and the Scope of the *Gramm-Leach-Bliley Act*

Dear Director Kraninger:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing to seek clarity for consumers and credit unions under the rules implementing the *Gramm-Leach-Bliley Act* (GLBA). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve nearly 120 million consumers with personal and small business financial service products. Credit unions are increasingly concerned with the imposition of multiple state laws regarding consumer privacy. NAFCU opposes the application of conflicting state privacy requirements to credit unions as they are already subject to the privacy requirements of the GLBA and serve as responsible stewards of sensitive consumer data. NAFCU supports a comprehensive federal data privacy standard that preempts state privacy laws while providing protections to consumers and clarity and consistency for credit unions (see attached NAFCU's Principles for a Federal Data Privacy Standard).

Many new state privacy standards contain exemptions for data covered by the GLBA, rather than institutions covered by the GLBA. NAFCU recognizes NCUA Chairman Rodney Hood's recent comments regarding the need for increased coordination and efforts among the Federal Financial Institutions Examination Council (FFIEC) members to respond to the burden on financial institutions posed by multiple privacy laws. The FFIEC should provide interagency guidance indicating that the GLBA should be the sole framework under which financial institutions collect, process, sell, or disclose consumer data, thereby eliminating duplicative state standards. NAFCU urges the CFPB to take the lead in mitigating the regulatory fragmentation created by states passing multiple, parallel regulatory frameworks.

NAFCU is encouraged by your efforts as Chairman of the FFIEC to promote collaboration and consistency in the supervision of all financial institutions. Cybersecurity and data privacy supervision are top concerns within the credit union industry. The cost of compliance with existing regulatory frameworks is already high; the cost of complying with countless different, and potentially competing, privacy standards is unsustainable. As a result, it is imperative that the

Bureau of Consumer Financial Protection

January 23, 2020

Page 2 of 2

FFIEC act swiftly to provide the industry with clear guidance as many financial institutions, particularly small, not-for-profit, community-based financial institutions like credit unions, may have difficulty complying with varying state standards.

The *California Consumer Privacy Act* (CCPA) and other proposed state privacy laws add new, parallel sets of obligations and standards for compliance, creating mounting and unnecessary compliance obligations for credit unions and confusion for consumers. As referenced, the CCPA's GLBA exemption does not exempt GLBA-regulated entities, only GLBA-regulated information. This leaves credit unions to establish two privacy frameworks: one for GLBA information and one for CCPA-covered information. When laws are passed in additional states, additional parallel frameworks will be necessary for each state where consumers may reside.

As these laws look at whether information is covered by the GLBA and its implementing regulations, the FFIEC should clarify in interagency guidance that all information collected and retained by credit unions and other financial institutions should be collected, processed, sold or disclosed pursuant to the GLBA. This would provide consistent protections for consumers across all states and minimize compliance burdens for credit unions and other financial institutions. If legally binding guidance were issued and all personal information were collected, processed, sold or disclosed pursuant to the requirements of the GLBA and Regulation P, that may satisfy the CCPA's exemption and reduce the number of parallel frameworks financial institutions must undertake. Without such guidance, credit unions are left in the dark to deal with the rise of state privacy legislation with no assistance from the FFIEC on how to approach compliance with these state laws and existing federal data privacy laws.

NAFCU's member credit unions support a uniform federal standard, not a patchwork of state privacy laws, to protect their member's data. Shifting state privacy requirements will undoubtedly result in undue burden for credit unions who already comply with the GLBA. The impact of privacy laws in varying jurisdictions will also have a chilling effect on the types of products and services credit unions are reasonably able to offer consumers. Accordingly, NAFCU supports a comprehensive federal privacy law that protects consumers, holds all entities accountable, and recognizes existing federal privacy laws that financial institutions follow.

Thank you for your consideration and attention to this important matter. NAFCU looks forward to working with you to address these concerns related to the scope of the GLBA for financial institutions. If you have any questions about this issue or if I may be of assistance to you in any way, please do not hesitate to contact me.

Sincerely,



B. Dan Berger
President and CEO

cc: The Honorable Rodney E. Hood, Chairman, National Credit Union Administration

The National Association of Federally-Insured Credit Unions (NAFCU) advocates for a comprehensive federal data privacy standard that protects consumers, harmonizes existing federal data privacy laws, and preempts state privacy laws. Credit unions are already subject to the *Gramm-Leach-Bliley Act* (GLBA) which requires financial institutions to disclose their privacy practices and to protect consumers' private information. The nationwide effect of the California Consumer Privacy Act (CCPA) and the rapid proliferation of state privacy legislation creates confusion for consumers and threatens unnecessary, duplicative compliance costs for credit unions. In light of the mounting uncertainty and escalating compliance burdens for credit unions, the need for federal privacy legislation is clear. NAFCU recommends that Congress consider federal privacy legislation that includes the following elements:

- 1. A comprehensive national data security standard covering all entities that collect and store consumer information.** *In order to protect consumers, retailers, fintech companies and any other organizations handling personal information should be required to provide reliable and secure information systems similar to those required of credit unions.*
- 2. Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.** *The patchwork of federal and state privacy laws creates an environment where consumers receive multiple disclosures on different information and their rights vary significantly across different types of organizations; this situation is confusing for consumers, burdensome for credit unions, and can only be resolved by a federal law that preempts state laws.*
- 3. Delegation of enforcement authority to the appropriate sectoral regulator. For credit unions, the National Credit Union Administration (NCUA) should be the sole regulator.** *Allowing NCUA, which is well versed in the unique nature of credit unions and their operations, to continue to examine and enforce any privacy and cybersecurity requirements is the most efficient option for both credit unions and American taxpayers.*
- 4. A safe harbor for businesses that takes reasonable measures to comply with the privacy standards.** *Any federal data privacy bill should provide for principles-based requirements based on an organization's specific operations and risk profile, and a safe harbor for organizations that design and implement appropriate measures.*
- 5. Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.** *Providing multiple privacy disclosures and opt-out mechanisms across multiple channels creates confusion for consumers and unreasonable burdens for credit unions. A new privacy law should incorporate the GLBA's requirements to avoid conflicting or duplicative disclosure requirements.*
- 6. Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.** *Actual damages to consumers are too difficult to establish by evidence and statutory damages for violations is incredibly ripe for frivolous lawsuits; sectoral regulators should have the power to assess scalable civil penalties, which can then be used to remedy and prevent consumer harm in a meaningful way.*