

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.*