SEPTEMBER 2022

NAFCU

ISSUE BRIEF

Data Privacy

EXECUTIVE SUMMARY

The current patchwork of state and federal data privacy legislation and regulation fails to meet the challenges of the contemporary data privacy risk environment. Risky data practices at insufficiently regulated businesses continue to leave Americans and their credit unions exposed to significant data privacy harms. The growing body of state data privacy legislation and regulation is not only inadequate to fully protect any American's data privacy but forces credit unions and other entities already subject to robust federal data privacy standards to form expensive parallel state data privacy compliance programs.

In this publication, the National Association of Federally-Insured Credit Unions (NAFCU) identifies six key principles that should guide the drafting of comprehensive federal data privacy legislation necessary to fully protect every American's data privacy and enable the credit union system to better serve its millions of members.

NAFCU strongly encourages Congress to enact comprehensive federal data privacy legislation that:

1. Recognizes the strengths and efficiencies of existing federal data privacy legislation and regulation and fully exempts credit unions and other federally insured financial institutions from new federal data privacy standards;
2. Expressly preempts all state data privacy legislation and regulation;
3. Vests exclusive rulemaking and discretionary enforcement authorities in covered entities' respective primary regulators;
4. Requires that all covered entities meet a robust information security standard;
5. Requires that all covered entities use uniform, easily-accessible data privacy disclosures; and
6. Establishes principles-based compliance safe harbors for covered entities taking reasonable steps to meet their data privacy responsibilities.

BACKGROUND

As of this NAFCU publication, and in just over four years, five states have passed comprehensive data privacy legislation. On June 28, 2018, then-California Governor Jerry Brown signed the California Consumer Privacy Act (CCPA) into law. During the November 2020 general election, California voters approved Proposition 24, or the California Privacy Rights Act (CPRA) as it is more commonly known. The CPRA strengthened Californians' CCPA data privacy rights and established the nation's first state-level data privacy regulator, the California Privacy Protection Agency (CPPA).

Comprehensive data privacy legislation in Virginia and Colorado followed shortly thereafter, signed into law in March and July 2021, respectively. Also in July 2021, the Uniform Law Commission, co-developer of the broadly adopted Uniform Commercial Code, approved the Uniform Personal Data Protection Act at its annual meeting. So far in 2022, comprehensive data privacy legislation has been signed into law in two more states, Utah in March and Connecticut in May. Similarly comprehensive data privacy legislation was considered in dozens of other states this year and should be expected to receive close attention again in January 2023, when most state legislatures will reconvene.

Of the five states that have passed comprehensive data privacy legislation, every state except California has fully exempted credit unions from its new data privacy standards based on credit unions' compliance with the robust data privacy standards contained in the Gramm-Leach-Bliley Act (GLBA) and the National Credit Union Administration's (NCUA) implementing regulations. In contrast, subsection 1798.145(e) of California's CCPA clumsily provided that the CCPA, "shall not apply to personal information collected, processed, sold, or disclosed pursuant to [the GLBA]." The CPRA amended this subsection to replace the qualifier "pursuant to" with the no clearer language "subject to". Due to a variety of factors, including the CPPA's failure to clarify which information the new California regulator believes is not "subject to" the GLBA, credit unions that have protected Californians' data for decades are required to form expensive parallel state data privacy compliance programs or risk exposing themselves to substantial compliance and litigation risks.

The preambles to most, if not all, states' comprehensive data privacy legislation remark that the adequate protection of Americans' data privacy requires that robust data privacy standards be applied across the entire economy, and not only within narrowly defined industries like financial services and healthcare. Considering how the data privacy risk environment has evolved and the European Union's General Data

Protection Regulation's (GDPR) international influence, this uniformity of states' opinions is unsurprising. NAFCU strongly agrees that businesses across the entire economy should be subject to robust data privacy and information security standards, like those contained in the GLBA.

For years, NAFCU has diligently made the case that data practices at insufficiently regulated businesses, including social media companies and uninsured financial technology companies, are rife with significant, avoidable data privacy risks that may cause Americans and their credit unions significant harm. Against this backdrop of ever-escalating data privacy risks and continued congressional inaction, it is no surprise that states are working to protect their citizens the best they can. However, the current patchwork of state and federal data privacy legislation and regulation is both insufficient to adequately protect any American's data across the entire economy and unnecessarily burdensome to credit unions and other federally insured financial institutions.

Fortunately, Congress has a rich history of efficiently protecting Americans' data privacy and understands the related value of robust information security standards. The most meaningful risks to Americans' data privacy have always surrounded the largest databases of Americans' most sensitive data – historically, those maintained by federal government agencies, financial institutions, and healthcare providers. The US Privacy Act of 1974 generally guarantees Americans have the right to access, correct, and control or prohibit certain uses and disclosures of their personal data maintained in most federal government agencies' databases. Under the Right to Financial Privacy Act of 1978, a government authority generally may not access a financial account holder's data held by a financial institution without first obtaining a subpoena and affording the account holder an opportunity to object. The use, disclosure, and safekeeping of Americans' most sensitive health data is regulated in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). And the Financial Services Modernization Act of 1999, as the GLBA is officially titled, and its implementing regulations together define the robust data privacy and information security standards applicable to credit unions and other financial institutions.

When the GLBA, HIPAA, and other existing federal data privacy legislation were passed, they met the most pressing data privacy challenges of their day, and, within their industries, they have evolved to meet today's most pressing data privacy challenges as well. However, it is obvious that the strength and efficiencies of federal data privacy legislation can no longer remain sequestered in narrowly defined industries. Today's data privacy risk environment is defined in large part by advances

in commercial data collection and data use technologies and Americans' near-constant engagement with an ever-growing number and variety of insufficiently regulated businesses.

Data privacy risks arising within insufficiently regulated businesses do not evaporate at states' borders. So no matter how forcefully any state may attempt to protect its citizens, no American's data privacy is protected across the entire economy. And, as the body of state data privacy legislation and regulation continues to grow and contort, credit unions face being forced to form potentially dozens of expensive parallel state data privacy compliance programs despite already being subject to the GLBA's robust federal data privacy standards.

Simply put, it is imperative that Congress act purposefully and thoughtfully to pass comprehensive federal data privacy legislation that ensures every American's data privacy will be adequately and efficiently protected across the entire economy and the credit union system is able to better serve its millions of members.

PRINCIPLES

NAFCU strongly encourages Congress to enact comprehensive federal data privacy legislation consistent with the following six key principles:

1. Comprehensive federal data privacy legislation should recognize the strengths and efficiencies of existing federal data privacy legislation and regulation and fully exempt credit unions and other federally insured financial institutions from new federal data privacy standards.

There are now greater and more varied risks to Americans' data privacy than there were last century, last decade, last year, and, even, last month. And, while many, if not most, of today's observable data privacy risks arise in industries not yet subject to any federal data privacy standards, federal data privacy legislation and regulation are not new concepts. As described above, Congress and federal regulators have successfully protected Americans' data privacy within various narrowly defined industries for nearly 50 years. Clearly, by choosing to protect Americans' data privacy in this piecemeal fashion, Congress allowed data privacy risks in other parts of the economy to grow and multiply. But, by passing certain industry-specific data privacy legislation, Congress laid the cornerstones of durable, responsive, and efficient federal data privacy frameworks that should serve as models for the comprehensive federal data privacy legislation needed today.

For example, through the GLBA, Congress helped define robust federal data privacy and information security standards for the financial services industries. Congress also provided the NCUA and other federal financial regulators the tools with which to efficiently build upon the GLBA's strengths. Through its regulation of thousands of credit unions across the country, the NCUA gains deep insights into credit unions' activities, risk centers, and risk management resources. With these deep credit union system insights, the NCUA is able to tailor its GLBA-implementing regulations and enforcement to meet all data privacy risks arising within the credit union industry without resorting to inefficient one-size-fits-all standards. Furthermore, because the GLBA enables the NCUA to research and respond to new data privacy risks arising within the credit union system, the NCUA can act, and has acted, to meet new data privacy challenges far more quickly than Congress can act.

Because existing federal data privacy legislation already provides the regulators responsible for their implementation with the tools necessary to meet all existing and new data privacy risks within their respective industries, credit unions and other federally insured financial institutions should be fully exempted from new federal data privacy standards. From all appearances, the majority of federal lawmakers appear to recognize the strength and efficiencies of the GLBA and the value of regulator-led regulation and understand that credit unions should be exempted from new federal data privacy standards. However, the appropriate scope of a GLBA exemption and other similar statutory exemptions appears to be an unsettled issue.

The obvious trend in statehouses, both those controlled by Democrats and those controlled by Republicans, is to fully exempt credit unions from new data privacy standards. Nonetheless, some federal lawmakers from both parties appear happy to buck this trend and needlessly subject credit unions to duplicative federal data privacy standards. The American Data Privacy and Protection Act (ADPPA), as written, would only provide credit unions with a far inferior information-level GLBA exemption. Under the proposed information-level GLBA exemption, credit unions would be subject to the ADPPA's new federal data privacy standards with respect to all data and data practices not "subject to" the GLBA. As credit unions serving Californians can attest, the regulatory relief available under such an information-level GLBA exemption is, in operation, arguably only illusory.

Qualifying language such as "pursuant to" and "subject to" has historically proven fertile ground for meaningful differences of opinion among federal courts. As case law surrounding other federal consumer protection legislation, such as the Telephone Consumer Protection Act (TCPA), makes clear, differences of opinion among federal

courts can quickly lead to applications of well-intentioned legislation that are anything but uniform. Furthermore, if comprehensive federal data privacy legislation provides that individuals may pursue private rights against covered entities and/or allows for state enforcement of new federal data privacy standards, the magnitude of risks to credit unions arising from inaccurate and conflicting federal case law multiplies.

If Congress fails to recognize the strengths and efficiencies of existing federal data privacy legislation and regulation and does not fully exempt credit unions from new federal data privacy standards, credit unions will find themselves immediately and unnecessarily exposed to new and substantial compliance burdens and legal risks despite their and the NCUA already meeting data privacy risks within the credit union system head-on and in timely fashion.

2. Comprehensive federal data privacy legislation should expressly preempt all state data privacy legislation and regulation.

As argued above, Congress must fully exempt credit unions and other federally insured financial institutions from new federal data privacy standards if it is to avoid inadvertently subjecting them to duplicative federal data privacy standards. But, if Congress is to also avoid perpetuating the current patchwork of state and federal data privacy legislation and regulation, Congress must also leverage comprehensive federal data privacy legislation to expressly preempt all state data privacy legislation and regulation.

To gain a fuller appreciation of the avoidable deficiencies inherent in the current patchwork of state and federal data privacy legislation and regulation, let's consider a Los Angeles lineman's data privacy. If the lineman belongs to a federally insured credit union, the lineman should take comfort in knowing her trusted financial institution is required to meet the GLBA's robust data privacy standards. If the lineman's credit union serves 50,000 or more Californians, her credit union may also be a covered entity under the CCPA with respect to her personal data and its data practices not "subject to" the GLBA.

However, even if one could divine with absolute certainty that there is some data that a credit union collects, processes, or discloses that is not subject to the GLBA, and therefore not already subject to robust federal data privacy standards, this textual justification buckles under scrutiny. Credit unions do not apply the GLBA's robust data

privacy standards to some data and lesser standards to other data. Credit unions apply the GLBA's robust data privacy standards across their entire data ecosystems.

Back to the Los Angeles lineman – what are the data privacy implications of her using her credit union debit card to purchase a toolbelt from a neighborhood hardware store? Or using her credit union debit card to book her next vacation at a hotel in nearby Las Vegas, Nevada? Each year, these and millions of other U.S. businesses together collect the names, physical and email addresses, phone numbers, dates of birth, credit and debit card details, geolocations, IP addresses, and more from hundreds of millions of Americans.

Unfortunately for the lineman, chances are that neither the neighborhood hardware store, because of its modest customer base, nor the multi-billion-dollar Las Vegas hotel, because of its location, is currently subject to any state or federal data privacy or information security standards – even in California. Therefore, it is likely neither business has any statutory duty to protect the lineman's data privacy.

So, while the GLBA's robust data privacy standards ensure the lineman's nonpublic personal information is safe within the confines of her credit union, the lineman's data privacy remains vulnerable at the dozens or hundreds of insufficiently regulated businesses with which she engages each year. Furthermore, even if a state could fully resolve all data privacy risks arising within its borders, the state would still not be able to fully protect any citizen's data privacy across the entire economy because no state is capable of adequately addressing many of the most meaningful data privacy risks that arise beyond its borders but nonetheless impact its citizens.

Not only will state data privacy legislation and regulation forever fail to adequately protect any American's data privacy across the entire economy, but state data privacy legislation, like the CCPA, and implementing regulation force credit unions already subject to robust federal data privacy standards to form expensive parallel state data privacy compliance programs. Presently, it is conceivable that credit unions could shortly become subject to new state data privacy standards in dozens of states. However, whether a credit union is forced to form an expensive parallel data privacy compliance program in one or 50 states, the simple fact remains that, until Congress expressly preempts all state data privacy legislation and regulation, credit unions are and will continue to be unnecessarily deprived of valuable resources better spent serving their members and communities.

3. Comprehensive federal data privacy legislation should vest exclusive rulemaking and discretionary enforcement authorities in covered entities' respective primary regulators.

Some have argued that, as to all covered entities, comprehensive federal data privacy legislation should vest rulemaking and enforcement authorities in a single federal regulator, perhaps the Federal Trade Commission (FTC). As to covered entities that do not presently have a primary regulator, e.g. international social media conglomerates and uninsured financial technology companies, the vesting of comprehensive federal data privacy rulemaking and enforcement authorities in a single federal regulator is logical and may provide the most direct path to responsible federal agency headcounts and budgets.

However, if credit unions and other federally insured financial institutions are not fully exempted from new federal data privacy standards, comprehensive federal data privacy legislation should vest exclusive rulemaking and discretionary enforcement authorities in their respective primary regulators. To do otherwise would not only unnecessarily complicate credit unions' and other federally insured financial institutions' existing data privacy compliance programs but would inefficiently inflate federal agency headcounts and budgets by tasking multiple agencies with overseeing data privacy risks within the same covered entities.

While Congress has previously vested federal data privacy rulemaking and enforcement authorities in a single federal regulator, such as the Department of Health and Human Services under HIPAA, Congress has bifurcated federal data privacy rulemaking and enforcement authorities where it was appropriate to do so. Congress did not task a single federal agency with implementing and enforcing the GLBA. Though the GLBA rightly respects the NCUA as federally insured credit unions' primary regulator, the Federal Deposit Insurance Corporation, Federal Reserve Board, the Office of the Comptroller of the Currency, and other agencies play active roles in the GLBA's implementation and enforcement within their respective financial industries.

As stated throughout this NAFCU publication, comprehensive federal data privacy legislation should fully exempt credit unions and other federally insured financial institutions from new federal data privacy standards. However, if Congress provides credit unions only a far inferior information-level GLBA exemption from new federal data privacy standards, Congress should vest exclusive rulemaking and discretionary enforcement authority, as to covered federally insured credit unions, in the NCUA. In

addition to the NCUA's decades of experience implementing and enforcing the GLBA within the credit union system, the NCUA's granular credit union knowledge and the NCUA's structure as an independent agency position it as the regulator most capable of effectively and efficiently implementing new federal data privacy standards within the credit union system.

For the same reasons, the NCUA is best positioned to effectively redress data privacy risks realized within the credit union system. In most cases, any harm an individual suffers following a data breach or other realized data privacy or information security risk is too far removed from a specific incident for the individual to reasonably establish a causal link between the harm suffered and the realized risk. However, if Congress fails to preclude private rights of action and state enforcement of new federal data privacy standards, the financial resources credit unions and other federally insured financial institutions will be forced to expend defending even plainly frivolous claims will be staggering. The NCUA's experience implementing and enforcing the GLBA's robust data privacy standards makes clear that the NCUA is best positioned to afford individuals harmed by any noncompliance within the credit union system adequate redress without inefficiently inflating compliance costs across the credit union system.

4. Comprehensive federal data privacy legislation should require that all covered entities meet a robust information security standard.

The value of Americans' data increases in lockstep with the number and variety of uses, beneficial and nefarious, to which it may be put and, as such, it must be robustly secured at all times. Credit unions must comply with the robust information security standard defined in the GLBA's Safeguards Rule. However, as seen above in the example of the Los Angeles lineman, no similar state or federal information security standard applies to millions of other U.S. businesses that together collect sensitive personal data from hundreds of millions of Americans each year.

Each year, data breaches at insufficiently regulated businesses not yet subject to any state or federal information security standard affect hundreds of millions of Americans and their credit unions. Criminals gaining unauthorized access to email accounts, commercial databases, and social media networks pilfer much more than usernames and passwords, and criminal targets are hardly limited to the most modest businesses. Notable data breaches at Microsoft, Equifax, Meta Platforms (formerly Facebook), and other household names involved information at the heart of successful existing federal

information security standards – names, dates of birth, social security numbers, and financial account details.

As stated previously, NAFCU strongly believes that until businesses across the entire economy are held to a robust information security standard, risks to Americans' data privacy can only be expected to grow and multiply. When Congress and federal regulators are developing federal information security standards for the broader economy, they should look to existing, time-tested federal information security standards, including those found in the GLBA's Safeguards Rule.

5. Comprehensive federal data privacy legislation should require that all covered entities use uniform, easily-accessible data privacy disclosures

Informed decision-making has long been a core tenet of effective consumer protections. In many ways, however, covered entities providing individuals too much information or information in too technical language can impair individuals' ability to make informed decisions just as severely as covered entities providing individuals too little information. Federal regulators charged with implementing comprehensive federal data privacy legislation within their industries should be made to develop and to require their covered entities to use uniform, easily-accessible data privacy disclosures.

Where reasonably possible, federal regulators should endeavor to tailor such uniform, easily-accessible data privacy disclosures to covered entities' respective industries. Neither the Truth in Lending Act (TILA) nor the Real Estate Settlement Procedures Act (RESPA) bears directly on data privacy or information security issues; however, the successes of the property settlement Closing Disclosure under the Consumer Financial Protection Bureau's TILA-RESPA Integrated Disclosure (TRID) rules provide perhaps the best illustration of how strongly individuals' autonomy and wellbeing can be supported by covered entities' use of well-tailored, uniform, easily-accessible disclosures.

6. Comprehensive federal data privacy legislation should establish principles-based compliance safe harbors for covered entities taking reasonable steps to meet their data privacy responsibilities.

Prescriptive, one-size-fits-all regulatory compliance and enforcement frameworks almost invariably produce severe, inefficient misalignments between the compliance

burdens borne by a regulation's most modest covered entities and the related risks inherent in their organization and operation. Contrastingly, principles-based regulatory compliance safe harbors, like that found in Part 748 of the NCUA's regulations, acknowledge and respect the meaningful differences in risk profiles that can exist even among covered entities within a narrowly defined industry.

Federal regulators charged with implementing comprehensive federal data privacy legislation within their industries should be made to establish regulatory compliance frameworks under which their covered entities are required to routinely self-assess for data privacy and information security risks and implement compliance programs and procedures proportionate to their individually-identified risks. By establishing principles-based regulatory compliance safe harbors for covered entities taking reasonable steps to meet their data privacy and information security responsibilities, regulators will ensure risks within individual covered entities are effectively managed without inefficiently inflating compliance costs across entire industries.