NAFCU'S PRINCIPLES FOR A FEDERAL DATA PRIVACY STANDARD

NAFCU

National Association of Federally-Insured Credit Unions

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Association of Federally-Insured Credit Unions (NAFCU) advocates for a comprehensive federal data privacy standard that harmonizes existing federal data privacy laws, preempts state privacy laws, and protects consumers. In this paper, NAFCU explains why such a standard is preferable to the growing piecemeal approach to privacy laws by first outlining its principles, then examining the existing landscape of privacy laws, the impact of the European Union's GDPR on the US credit union industry, the nationwide effect of the California Consumer Privacy Act, and the rapid proliferation of state privacy legislation. Much like credit unions, credit union service organizations (CUSOs) may also have to comply with multiple state privacy laws and the GDPR.

In light of the mounting uncertainty and rising compliance burdens from federal and state regulators, the need for federal privacy legislation is clear. Considering federal legislative efforts up to this point and the legal authority supporting a nationwide federal privacy standard, NAFCU is taking the lead in advocating for the uniformity in the application of privacy laws through a comprehensive national standard. NAFCU recommends 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.
2. Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.
3. Delegation of enforcement authority to the appropriate sectoral regulator. For credit unions, the National Credit Union Administration (NCUA) should be the sole regulator.
4. A safe harbor for businesses that takes reasonable measures to comply with the privacy standards.
5. Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.
6. Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.

INTRODUCTION

NAFCU supports comprehensive federal privacy legislation because credit unions want a uniform standard that is workable for their institutions and implements proper guardrails for consumers' protection into the entire environment rather than certain sectors. Relatedly, NAFCU continues to advocate for the adoption of national data and cybersecurity standards for all entities that collect and store consumer information. Federal law establishes certain standards for financial institutions, including credit unions, to notify consumers how their personal information is being shared with vendors

and other third parties. Unfortunately, the current landscape does not apply equally to all players in the market—leaving consumers vulnerable to data breaches by sophisticated hackers. Considering data is now the world's most valuable asset, Congress should take steps to protect consumers' data. Congress has yet to establish a national data privacy standard and as a result, some states have taken matters into their own hands. data breaches by sophisticated hackers. Considering data is now the most valuable asset in the world, Congress must take steps to protect consumers' data. Congress has yet to establish a national data privacy standard and as a result, some states have taken matters into their own hands.

As states move to implement their own privacy laws, conflicting requirements and consumer rights are already creating confusion and leading to daunting compliance considerations. Differences in state laws are particularly important with respect to *who* is protected, what constitutes a data breach, and *how* credit unions must establish processes and procedures to handle consumer data. These questions are critical for those credit unions operating across state lines; and credit unions of all sizes are beginning to understand the massive systems overhaul necessary to comply with potentially 50 different laws as well as the potential legal implications of violating these laws. NAFCU aims to prevent such a result by proposing a uniform standard that preempts state privacy laws and establishes certainty for credit unions across the country.

California will soon implement the nation's most comprehensive data privacy law—the California Consumer Privacy Act (CCPA). Other states are not far behind, with some taking an approach similar to that of the European Union's (EU's) General Data Protection Regulation (GDPR). In addition to state privacy laws, credit unions may need to assess whether the EU's GDPR—which places stricter privacy standards related to personally identifiable information—applies to the information they collect, hold, transfer or process. In order to avoid risk of litigation, it is important that credit unions understand the impact of privacy laws in varying jurisdictions and how those requirements compare to the GDPR and the Gramm-Leach Bliley Act of 1999 (GLBA).

Congress should act now because current and proposed state-specific privacy laws not only neglect to fully protect consumers, but also stifle innovation and economic growth for institutions—especially for credit unions, who continue to serve low- and moderate-income individuals and underbanked communities. Congress does not need to start anew to create a federal privacy standard. Instead, NAFCU encourages Congress to look to existing federal privacy laws to build a strong federal data privacy standard. For credit unions, the GLBA exists to serve as the primary data protection regulation

that requires institutions to explain how they share and protect consumers' private information.

A federal data privacy law should not be structured as one-size-fits-all; NAFCU continues to advocate that all federal regulations recognize the unique nature of credit unions and provide exemptions and tailored provisions to minimize resource and compliance burdens. Effective federal data privacy legislation should recognize the nuances among the different types of information collection and the various industries collecting consumer information. As such, Congress should consider existing federal laws, like the GLBA, to create a data privacy framework that protects consumers and enables businesses to effectively protect the information they collect. NAFCU will be the leader in advocating for uniformity in the form of a federal data privacy standard to provide clarity and certainty to the credit union industry.

NAFCU'S PRINCIPLES FOR A COMPREHENSIVE DATA PRIVACY STANDARD

In proposing a national data privacy standard, Congress should extend privacy and data security requirements to the entire environment. At the same time, Congress must recognize the success of existing federal privacy laws and build a framework around those existing laws that both protects consumers and eliminates the unnecessary compliance burden. NAFCU encourages Congress to adopt the following six principles as foundational blocks to form a strong, federal privacy law:

1. A comprehensive national data security standard covering all entities that collect and store consumer information.

Credit unions and non-financial institution entities should be held to the same standard with respect to privacy and data security obligations. With the increase in the value of data in our economy, those who use data have more motivation to engage in unethical practices. Consumers are more conscientious about how their data is shared and with whom. The internet has transformed our economy in such a way that there is no longer a valid reason to impose privacy requirements only on specific sectors. General obligations to inform consumers of their rights and ensure the privacy of consumer data should be consistent across the country and apply to any organization that gathers personal information about consumers.

Further, the security of consumer data is the responsibility of all parties that handle such data, and all parties should be held equally accountable for their practices. Merchant data

breaches continue to be a source of huge losses for consumers.[1] In a recent member survey, NAFCU found that 82 percent of credit union respondents were impacted by a local merchant breach within the past two years.[2] However, while credit unions and other financial institutions comply with strong data and cybersecurity standards, retailers and merchants lack similar standards.

A federal privacy standard should include a data security provision that requires retailers and others handling personal and financial information to provide reliable and secure information systems, similar to those required by credit unions. The provision should specifically require a data breach notification requirement for all entities. Further, to protect consumers, where unencrypted financial account information is subject to infiltration, the provision should require organizations to notify any financial institution holding those accounts of the breach to ensure that security risks can be contained and mitigated as quickly as possible.

There is no reason that a small credit union should be subject to more stringent requirements than an organization like Equifax, or that an organization like Facebook should not be subject to any requirements. Similar data security requirements should be imposed for fintech companies, retailers, and other entities that handle personal and financial information. Those who seek unauthorized access to consumer data will find the easiest point of entry into our interconnected system. Consumers are only truly protected when all parties, not just financial institutions, are responsible for protecting their personal and financial information and bear the cost of a data breach

2. Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.

A comprehensive federal consumer privacy law should harmonize existing federal laws that deal with the handing of personal information, including maintaining an exception that permits the sharing of information to assist government or law enforcement inquiries. The harmonization of existing federal laws would ensure that federal laws dealing with the handling of personal information are not overlapping and contradictory.

---

1 Dennis Green & Mary Hanbury, "If you shopped at these 16 stores in the last year, your data might have been stolen," Business Insider (Aug. 22, 2018).

2 NAFCU, Economic & CU Monitor (October 2018).

In a 2012 report to policymakers and businesses entitled "Protecting Consumer Privacy in an Era of Rapid Change,"[3] the FTC recognized the concern regarding potentially inconsistent privacy obligations for businesses and thus recommended that a new federal privacy legislation should not impose overlapping or duplicative requirements on conduct that is already regulated.[4] That report was issued the same year as the proposal for the GDPR, but the legal environment has only become significantly more complex and duplicative in the intervening years. In particular, the report urged Congress to harmonize any privacy legislation with the GLBA.[5] Moreover, a federal privacy framework should include a safe harbor provision similar to that included in the Bank Secrecy Act (BSA), which was intended to shield financial institutions, their officers and employees from civil liability for reporting known or suspected criminal offenses or suspicious activity to a government agency.[6] A new federal privacy standard should explicitly indicate that financial institutions that comply with existing federal laws related to the handling of personal information (as enumerated in the law) would not be liable under the federal privacy law.[7]

Moreover, analogous to the GDPR in Europe, the purpose of a federal privacy standard is to synthesize the current patchwork data protection laws under a uniform national standard. Credit unions must be able to effectively serve their members across jurisdictions and should not be exposed to the unnecessary compliance burdens of 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 Fair Credit Reporting Act all have some state preemption provision.[8] The CAN-SPAM Act preempts state laws that expressly regulate the use of email to send commercial messages, with a narrow exception.

---

3 *See generally*, FTC, "Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers" (March 2012).

4 *Id.*

5 *Id.* at 16-17.

6 31 U.S.C. §5318(g)(3)(A).

7 *Id.*

8 *See* 15 U.S.C. §§ 6501–6506; 15 U.S.C. §§ 7701-7713; 15 U.S.C. § 1681t(a).

This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.[9]

Similarly, a federal data privacy standard should preempt any state law that expressly regulates data privacy. The purpose of privacy and cybersecurity laws are only achievable if the protections put in place are both comprehensive and consistent. A federal privacy law without preemption would be ineffective in resolving the current issues posed by a patchwork of state privacy laws. Without consistent cybersecurity 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. Ultimately, without preemption, a federal privacy law simply becomes the 51st law that requires the compliance of credit unions.

3. Delegation of enforcement authority to the appropriate sectoral regulator. For credit unions, the NCUA should be the sole regulator.

As discussed in the Rulemaking and Enforcement section below, 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 serves as the primary regulator for credit unions since its inception. In addition to the institutional knowledge of credit unions, the current structure of the NCUA as an independent agency, including a three-person board, has been effective in regulating credit union activities for decades. As such, in the area of privacy enforcement, the NCUA should be the sole 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.

4. A safe harbor for businesses that take reasonable measures to comply with the privacy standards.

Any federal data privacy bill should provide for principles-based requirements and offer a safe harbor for businesses that take the appropriate steps to comply with the law.

---

9 *See* 15 U.S.C. § 7707(b)(1).

For example, the guidelines in NCUA's Part 748 requires 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.

Any organization 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. Providing a safe harbor for those businesses that take such measures to safeguard consumer data will be beneficial for both businesses and consumers as the safe harbor incentivizes businesses to safeguard sensitive consumer data.

5. Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.

The GLBA and its implementing regulation, Regulation P, already mandate that financial institutions provide their customers with initial and annual notices regarding those institutions' privacy policies. In certain circumstances, Regulation P permits financial institutions to qualify for an exemption that does not require them to send annual privacy notice, but only if the policies have not changed since the prior year. These disclosure requirements are already quite rigorous; the content requirements of the CCPA's initial notice as set out in the proposed regulations do not differ in any substantive way from GLBA's requirements except with regard to specific notices as to the consumer's rights under California law.[10] A new privacy law should incorporate the GLBA's privacy mandate so that financial institutions, including credit unions, do not have to be subject to conflicting or duplicative privacy requirements.

6. Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.

Any remedy for noncompliance with a federal privacy standard should be appropriately tailored to provide consumers a right to reasonable redress for the harm caused.

---

10 California Department of Justice, Notice of Proposed Rulemaking Action, Cal. Code Regs. tit. 11, § 999.305(b).

Historically, the two methods of directly compensating consumers for harm are (1) assessing actual damages and (2) establishing damages by statute; however, neither one is appropriate for privacy violations.

Any material harm consumers suffer as a result of the breach of privacy is often far removed from a specific incident to legally establish that the breach was the cause of the harm. In other words, it is very difficult to tie a specific privacy violation to an individual consumer's stolen identity or unauthorized transactions. It is very rare that a consumer is able to establish that a particular action by an organization caused them a specific injury beyond the initial actions taken to secure their information in the aftermath of a breach.

This issue is sometimes addressed through statutory damages. However, statutory damages for violations is incredibly ripe for abuse, especially as breaches can be suffered even when an organization has taken all the appropriate steps. The Telephone Consumer Protection Act (TCPA) is an example of flagrant misuse of a statutory private right of action.[11] Because the statute allows for a private right of action without any actual injury, the TCPA has become fertile ground for frivolous lawsuits that has proven to be ineffective in providing the necessary relief for consumers. From 2010 to 2016, the number of TCPA lawsuits has increased by 1,272 percent, with plaintiffs' attorneys receiving millions of dollars in compensation against legitimate businesses.[12] As plaintiff attorneys benefit from multi-million dollar attorneys' fees, an individual consumer in these class action lawsuits often receives only a nominal award.[13]

The application of privacy and security laws is complex in scope and level of application, so the appropriate sectoral regulator has the industry-specific expertise to serve as the sole enforcer of the federal privacy law for entities within its authority. Expert regulators have the bandwidth and power to shape and balance good policy with consumer protection. For this reason, the appropriate remedy for violations of a national privacy standard is for a regulator to make a decision about how to use civil fines to compensate consumers, based on the facts and circumstances related to a particular violation. Accordingly, the NCUA is best suited to monitor and enforce a federal privacy law within the credit union industry.

---

11 47 U.S.C. § 227 (b)(3), (f)(1). The TCPA provides a private right of action for violations and statutory damages in the amount of $500 for each separate violation and up to $1,500 for each "willful" violation.

12 *See* Institute for Legal Reform, "TCPA Litigation Continues to Skyrocket; 1,272 Percent Increase Since 2010," U.S. Chamber Institute for Legal Reform. (Jan. 27, 2017).

13 Josh Adams, "The Imperative to Modernize the TCPA: Why an Outdated Law Hurts Consumers and Encourages Abusive Lawsuits," ACA International (June 2016).

THE CURRENT STATE OF U.S. FEDERAL PRIVACY LAW AND ITS IMPACT ON CREDIT UNIONS

Currently, there is no federal law that generally governs the privacy of consumer information in the United States. Historically, federal privacy laws have been established with regard to individual sectors to address especially sensitive information or specific kinds of privacy harms. Because financial institutions necessarily collect and retain highly sensitive information regarding consumer's financial accounts and activities, Congress has passed two significant laws that specifically address the privacy of information in the financial sector: the Gramm-Leach-Bliley Act and the Right to Financial Privacy Act.

Gramm-Leach-Bliley Act (GLBA): The GLBA is the primary federal law governing data privacy for credit unions. The GLBA contains two significant rules: the Financial Privacy Rule[14] and the Safeguards Rule.[15] The Consumer Financial Protection Bureau (CFPB) implements the GLBA's[16] Financial Privacy Rule in Regulation P,[17] which generally prohibits sharing private financial information with nonaffiliated third parties without appropriate disclosures. The NCUA implements the GLBA's Safeguards Rule in Part 748 of its regulations[18] which requires credit unions to appropriately safeguard member information against unauthorized access. Below is a brief summary of each:

- ***Regulation P:*** The regulation sets forth the rules that govern a credit union's duty to provide notices and limit its disclosure of non-public personal information, which includes personally identifiable information collected about a consumer in connection with providing a financial product or service. A credit union must disclose its policy for sharing and gathering nonpublic personal information to new members, and to all members on an annual basis. Regulation P maintains a general prohibition against sharing nonpublic personal information with third parties, absent providing the consumer with proper disclosures and the ability to opt out of such sharing. If a credit union changes its policies and practices regarding disclosures to third parties, it must revise its privacy and opt out notices.

14 15 USC §6802.

15 15 USC §6801.

16 *See* 4 Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, Title X, 124 Stat. 1983 (2010) (The Dodd-Frank Act transferred rulemaking authority for most provisions of Subtitle A of Title V of the GLBA to the CFPB for financial institutions and other entities under the CFPB's jurisdiction).

17 *See* 12 CFR Part 1016.

18 *See* 12 CFR Part 748.

› ***Part 748 Security Program:*** The GLBA requires the NCUA to establish administrative, technical and physical standards for the protection of customer records and information. These standards are implemented in Part 748 and require credit unions to maintain the security and confidentiality of customer information, and to protect against any anticipated threats or hazards to the security or integrity of such records. The NCUA requires all credit unions to have a response program that can be implemented to address incidents of unauthorized access to member information. Appendix B to Part 748 provides more detail on the requirements of the program. Most importantly, credit unions are required to notify members where misuse of the information has already occurred or is reasonably possible.

The Right to Financial Privacy Act (RFPA):[19] This law became effective on March 10, 1979,[20] and acknowledges that financial institution customers, including credit union members, have a right to expect that their financial activities will have a reasonable amount of privacy from federal government scrutiny. Any government agency that obtains, or any credit union or credit union employee who discloses information in violation of the RFPA could be liable for damages or other litigation-related expenses.

The GLBA and RFPA are mature, developed frameworks around which financial institutions have established privacy policies, disclosure procedures and sophisticated, risk-based systems of safeguards to protect this information. The GLBA, which has been in place for two decades, requires disclosure of privacy policies, opportunities for consumers to opt-out of having their information shared, and a requirement that information be maintained such that it remains accurate and confidential. These laws and implementing regulations were written specifically for financial institutions and, in some areas, are not as comprehensive as the state-level laws either already passed or likely to be proposed in the future.

As Congress looks ahead to legislating in this arena, it should recognize the strengths and successes of preexisting legal frameworks. A strong general data privacy standard would better protect consumers by allowing already-regulated sectors, including credit unions, to continue to operate under existing laws and regulations where they are sufficient. Additionally, a comprehensive federal data privacy standard should supplement those existing frameworks where necessary to ensure that consumers receive the same level of protection across all sectors. Ensuring new legislation complements

19 12 USC §3401 *et seq.*

20 Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, Title XI, 92 Stat. 3697 (1978).

and supplements existing frameworks wherever possible balances consumer protection needs against the monetary cost and implementation burden for credit unions and other financial institutions.

THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION (GDPR)

Outside of the United States, other nations are passing privacy legislation at twice the rate of previous years.[21] Internationally, the EU's GDPR is the most comprehensive data privacy law that may impact credit unions and CUSOs. On May 25, 2018, the GDPR established a privacy framework that applies to organizations in all member-states and some organizations outside of the EU's borders. Organizations are covered by the GDPR if they offer a product or service to persons within the EU or if the organization tracks behavior of an individual who is physically located in the EU. The GDPR claims jurisdiction over any organization that meets this coverage test, regardless of whether the organization is physically located in the EU.[22]

The protections of the regulation apply to data regarding any natural person within the EU's legal borders, regardless of citizenship or residency.[23] The GDPR refers to these individuals currently within the borders of the EU as "data subjects," and grants these data subjects with eight rights regarding their data. These eight rights include (1) the right to basic information about what information is collected and shared;[24] (2) the right of access to the data collected about that subject;[25] (3) the right to rectification of any errors in the data about that subject;[26] (4) the right to erasure of data that no longer serves its purpose;[27] (5) the right to restrict processing of data about a subject;[28] (6) the right to object to processing of data for certain purposes;[29] (7) the right to data portability;[30] and (8) the right to not be evaluated solely on the basis of automated processing.[31]

21 Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2019 (August 1, 2019).
22 GDPR, Art. 3.
23 EU Regulation 2016/679 (GDPR), Art. 4(1).
24 GDPR, Art. 12-14.
25 GDPR, Art. 15.
26 GDPR, Art. 16.
27 GDPR, Art. 17.
28 GDPR, Art. 18.
29 GDPR, Art. 21.
30 GDPR, Art. 20.
31 GDPR, Art. 22.

Organizations are required to establish processes and procedures to give effect to these rights. They are also required to process data in accordance with data principles, including that data should be (1) processed lawfully, fairly and transparently; (2) collected and processed for a specific, explicit and legitimate purpose; (3) collected to the extent necessary to achieve that purpose; (4) maintained in an accurate state; (5) stored only as long as necessary to achieve that purpose; and (6) kept secure.[32]

Finally, the GDPR states that organizations should be held accountable for violations of these principles.[33] Credit unions that fail to comply with the GDPR's requirements may be subject to fines of up to 20 million Euros or four percent of a company's annual global turnover, whichever is higher. Further, the GDPR also creates a private right of action for "material or non-material damage" resulting from a violation of the GDPR.[34] Data subjects can sue organizations for alleged violations and seek damages for material harm (actual loss or loss of profits) and nonmaterial harm (emotional distress). Credit unions have been and continue to obtain expert assistance to assess whether they may be subject to the GDPR or the EU enforcement under international law and to what degree GDPR-compliance is appropriate for their institution.

THE GDPR'S IMPACT ON CREDIT UNIONS

Compliance with the GDPR depends on a credit union's individual operations and membership. Credit unions that who have made a determination that they are subject to the GDPR and a risk-based business decision to comply with the GDPR often have members who:

- Currently live in Europe;
- Are military personnel stationed in the EU (e.g., airman from the Air Force residing in Germany, even though a U.S. Citizen, would fall under GDPR protection); and
- Are EU citizens studying in the U.S.

However, serving members who live in or are citizens of the EU does not automatically require compliance with the GDPR—if a credit union does not meet the organizational scope of the rule (targeting products and services to people located in the EU or monitoring behavior of persons in the EU), then it may not be subject to the GDPR.

32 GDPR, Art 5(1).
33 GDPR, Art. 5(2).
34 GDPR, Art. 82.

Further, credit unions that might fall within the scope of the rule may make a risk-based business decision to delay compliance with the GDPR because it is not clear that an EU state has any jurisdiction to enforce foreign law against the credit union. These determinations involve conducting complex analyses of international law and jurisdiction that are often very expensive to obtain. A credit union who makes the determination that it must comply must achieve compliance, leading to further cost.

THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

On June 28, 2018, California Governor Jerry Brown signed the CCPA into law. The CCPA is the most comprehensive privacy law in the United States. Due to the size of California's population and the share of technology firms established in the state, the California law is widely viewed as a *de facto* national standard. The CCPA is set to become effective on January 1, 2020 and requires the California Attorney General (AG) to issue regulations within six months of the effective date, or by July 1, 2020. On October 11, 2019, the AG proposed regulations implementing the CCPA.[35]

The CCPA provides comprehensive data privacy measures for California consumers that includes enumerated consumer privacy rights. It also imposes obligations on "businesses," that meet designated thresholds, who collect or sell consumers' "personal information" to disclose how the consumer's information is being collected or sold.

A "business" as defined by the CCPA is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information or on behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California."[36] The entity must also satisfy one or more of the following thresholds:

- Annual gross revenue in excess of $25 million;
- Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or
- Derives 50 percent or more of its annual revenues from selling consumers' personal information.[37]

35 Cal. Reg. Notice Register, 2019, No. 41-Z, p. 1341 (October 11, 2019).
36 Cal. Civ. Code § 1798.140(c).
37 Cal. Civ. Code § 1798.140(c)(A)-(C).

The CCPA requires that covered businesses provide disclosures to consumers indicating what information will be collected and how it will be used. Disclosures must be made at or before the point of collection,[38] and further disclosures must be made on a covered business's website.[39] Under the CCPA, consumers have a "right of access" to their personal information, and covered businesses must respond to consumer requests to know what information is being kept and for what purpose.[40] A consumer also has the right to request a covered business delete their personal information.[41] The CCPA provides limited exceptions for instances when a covered business is not required to delete personal information after receiving a verifiable request. The CCPA provides consumers with the right to opt-out of the sale of personal information when a covered business is selling their personal information for economic gain.[42] A business must include a clear and conspicuous link on their website, titled "Do Not Sell My Personal Information."[43] Lastly, a consumer has the right to be free from discrimination when exercising their rights under the CCPA.[44] Potentially discriminatory acts could include charging a different rate, providing an inferior good or service, or denying access to goods and services because of a consumer's request. However, the CCPA does not prohibit offering a "financial incentive" for consumers to share their personal data.

The CCPA requires that covered businesses establish two or more designated methods for receiving requests to know or requests for deletion, including at minimum, a toll-free telephone number, and a website (if available).[45] A covered business must verify the identity of the requester, promptly disclose the identity of the requestor, then deliver the required information free of charge to the consumer within 45 days.[46] The disclosure period must cover the preceding 12 months.[47]

---

38 Cal. Civ. Code § 1798.100(b).
39 Cal. Civ. Code § 1798.130(a)(5).
40 Cal. Civ. Code §§ 1798.100 and 1798.115.
41 Cal. Civ. Code § 1798.105(a).
42 Cal. Civ. Code § 1798.120(a)
43 Cal. Civ. Code § 1798.135(a)(1).
44 Cal. Civ. Code § 1798.125.
45 Cal. Civ. Code § 1798.130(a)(1).
46 Cal. Civ. Code § 1798.130(a)(2).
47 Cal. Civ. Code § 1798.125 (d).

The CCPA defines "personal information" broadly. Information that identifies, relates to, or could reasonably be linked, directly or indirectly, with a particular consumer or household is covered by the rule. Some personal information may be exempt from some of the CCPA's provisions. Exemptions of particular use to credit unions include:

- ***GLBA Exemption:*** The CCPA exempts any personal information that is collected, processed, sold, or disclosed pursuant to the GLBA.[48]
- ***FCRA Exemption:*** The CCPA exempts personal information identifying a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is collected, maintained, disclosed, sold, communicated or used by a consumer reporting agency, by a furnisher of information, or by a user of a consumer report.[49]
- ***Business Individual Exemption:***[50] Personal information collected by a credit union while conducting a business transaction is exempt from much of CCPA, when a credit union collects data of a California resident who is conducting a transaction on behalf of a business. However, this exemption does not apply to the right to opt out of the sale of personal information, the right to be free from discrimination when exercising other rights, or the private right of action in the event of a data breach. Notably, this exemption expires after one year. After one year, individual contact information will be covered by the CCPA unless the California legislature takes further action in the interim.
- ***Employee Exemption:***[51] The rights to access, correct and opt-out of sale do not apply to employees, job applicants, owners, directors, staff, officers, contractors and medical staff ('employee"). However, businesses will still be required to meet the notice requirements laid out in Section 1798.100 and the private right of action still applies in the event of a data breach. This limited exemption expires after one year. In the event the California legislature fails to address employee data privacy by January 2021, employee information collected will then be subject to the full requirements of the CCPA.

PROPOSED CCPA REGULATIONS

The CCPA specifically instructs the AG to release implementing regulations to establish rules and procedures for several of the law's provisions and proposed regulations were

48 Cal. Civ. Code § 1798.145(e).
49 Cal. Civ. Code § 1798.145(d).
50 Cal. A.B. 1355 (2019-2020).
51 A.B. 25 (2019-2020).

released on October 11, 2019.[52] In the proposed regulations, the California AG considered and rejected the concept that the CCPA conflicts with other state regulations.[53] The California AG estimates compliance costs associated with CCPA regulations from 2020 to 2030 may total anywhere from $467 million to $16 billion.[54] Moreover, an assessment prepared by a research firm for the California AG estimates the total cost of initial compliance with the CCPA will be approximately $55 billion.[55]

Additionally, the AG rejected a "GDPR safe harbor" under the CCPA because the two laws have vast differences.[56] The CCPA is often compared to the GDPR; however, there are areas where the CCPA and GDPR diverge. Therefore, even credit unions who are striving to meet the GDPR's high bar will have to separately satisfy CCPA requirements, if they are subject to both rules. A table illustrating the differences between the two laws and the burden that results for these credit unions is contained in the Appendix to this paper.

The proposed regulations set forth requirements notifying consumers of information collection and the right to opt-out, including guidance for how to meet this requirement when the information is collected online versus offline.[57] Moreover, the proposed regulations provide examples of discriminatory practices and guidance on determining whether a "financial incentive" for sharing data is permissible. The proposal also provides further guidance on information that must be included in the CCPA-mandated privacy policy posted online.[58]

52 Cal. Civ. Code § 1798.185.

53 Cal. Reg. Notice Register, 2019, No. 41-Z, p. 1346.

54 California Department Of Justice, Office of the Attorney General, California Consumer Privacy Act (CCPA) Fact Sheet (*citing* Berkeley Economic Advising and Research, LLC, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations (Aug. 2019)).

55 California Department Of Justice, Office of the Attorney General, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations 10-11 (Aug. 2019).

56 *Id.*

57 California Department of Justice, Notice of Proposed Rulemaking Action, Cal. Code Regs. tit. 11, § 999.300 *et seq.*

58 See Cal. Code Regs. tit. 11, § 999.336.

Regarding consumer requests, the proposed regulations establish detailed timelines for processing requests, content requirements for responses and training requirements. The proposal also establishes verification procedures including:

- Implementing a verification system that takes into account data sensitivity;
- Authenticating a consumer's identity by providing specific guidance to non-account holders; and
- Issuing a blanket prohibition on disclosing specific sensitive data in response to a request.[59]

Notably, the proposed regulations provide additional guidance for responding to requests to opt-out; however, the proposed regulations do not impose any requirement on businesses to verify the consumer's identity regarding a request to opt-out. The proposed regulations do not clarify exemptions, applicability thresholds or the meaning of "sale" under the CCPA, leaving several important questions still open.

PRIVATE RIGHT OF ACTION

The CCPA imposes civil penalties for companies that fail to comply with the law. In addition to civil penalties, the CCPA has a narrow private right of action for data breaches. Notably, information subject to the exceptions enumerated in the CCPA will remain covered under CCPA's private right of action for security breaches.

The CCPA grants a private right of action to consumers when (1) a business experienced a security incident or data breach; and (2) the business failed to maintain *reasonable* security practices and procedure; the statutory damages ranges between $100 and $750 per consumer per incident or actual damages, whichever is greater.[60]

It is unclear what the statute considers "reasonable security measures." The statutory language establishing the carve-outs for financial information under the CCPA does not apply to the private right of action provision; consequently, credit unions, like all other businesses, are still liable for significant statutory damages in the event of a data breach. Credit unions have reason for concern if a breach occurs. The institution could see litigation based on the CCPA and face significant legal fees and potential damages.

59 Cal. Code Regs. tit. 11, § 999.300, et seq.

60 Cal. Civ. Code § 1798.150(a)(1).

It is important to note that the CCPA is not the only vehicle to exercise a private right of action for violation of the CCPA. In addition to the CCPA's private right of action, California residents have a private right of action option under the Unfair Competition Law (UCL).[61] California's UCL gives consumers the ability to sue businesses that have engaged in unlawful, unfair, or fraudulent acts.[62] Historically, the UCL has allowed Californians to enforce laws that do not provide for a private right of action. Although the CCPA provides that the statute "shall [not] be interpreted to serve as the basis for a private right of action under any other law," it is unclear whether the legislature specifically intended to preclude a private right of action under the CCPA.[63] The use of a private right of action clause in other laws to enforce the CCPA will likely be tested in California courts. Ultimately, credit unions that may be subject to the CCPA requirements should consult with their local attorney to develop a compliance plan that best limits exposure to CCPA claims.

THE CCPA'S IMPACT ON CREDIT UNIONS

Based on the plain language of the CCPA, its application to credit unions is not entirely clear. The CCPA's definition of a "business" includes organizations that operate for-profit. Credit unions are not-for-profit entities that operate for the financial benefit of their member-owners because of their nature as cooperative financial institutions. The question of whether the CCPA affects credit unions is complicated; however, several experts agree that credit unions fit within the definition of a "business" and must comply with the CCPA. Ultimately, the courts may have to determine whether credit unions are subject to the CCPA, but based on the language of the statute, California courts would likely reject a broader definition of "business" to exempt credit unions from compliance. Therefore, it appears credit unions could be deemed a "business" under the CCPA. In addition to credit unions, credit union service organizations (CUSOs) that meet the definition of a "business" under the CCPA will likely be required to comply with its provisions to the extent that they collect "personal information" that is not exempt in the rule.

The CCPA's GLBA carve-out language will be available for credit unions, though it is important to note that the exemption applies to specific information subject to the

61 2 Cal. Bus. & Prof. Code § 17200, et seq.
62 2 Cal. Bus. & Prof. Code § 17200.
63 Cal. Civ. Code § 1798.150.

GLBA, rather than to organizations covered by the rule. The CCPA provides:

> "This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code)."[64]

Notably, the GLBA's definition of "nonpublic personal information" is narrower than the CCPA's definition of "personal information," so it is possible that credit unions will collect information subject to the CCPA and not the GLBA. As such, federal credit unions may wish to evaluate the types of data they handle that fall within the CCPA definition of "personal information," but outside the GLBA definition of "nonpublic personal information," including (1) personal information of employees or contractors; (2) consumer contact lists purchased from third parties for marketing purposes; and (3) personal information associated with financial services or products that are not used primarily for personal, family, or household purposes. Further, even information included under the GLBA exception may still be subject to a personal right of action in the event it is breached.

Compliance with the CCPA is a significant undertaking and often includes conducting an inventory of all data held by the credit union. Credit unions typically then perform data mapping to identify where and how consumer information is held, received, transferred and used throughout the credit union. This is necessary to make proper disclosures, respond to requests for disclosure or deletion, or claim appropriate exceptions in response to such a request.

It also requires establishing internal procedures, appropriate websites and notices to comply with the law and the necessary mechanisms and communication channels for consumers to submit requests and exercise their rights under the CCPA. Credit unions must also establish appropriate trainings to ensure staff handle requests and opt-outs properly and use information in accordance with the credit union's policies and disclosures. Finally, credit unions must ensure agreements with third-party vendors and service providers provide sufficient protections for credit unions, limitations on sale and use of information regarding consumers potentially covered by the CCPA.

---

64 Cal. Civ. Code § 1798.145(e).

OTHER STATE LEGISLATIVE EFFORTS

Absent congressional action, a number of states are looking to provide data privacy protections for consumers in the form of either sector-specific or comprehensive laws. Legislation similar to the CCPA has been introduced in state legislatures across the country; however, many of those proposed bills failed to pass. For example, similar omnibus privacy bills have been introduced in Connecticut, Hawaii, Maryland, Massachusetts, Minnesota, New York, Pennsylvania, Rhode Island, Texas, and Washington. Maine and Nevada recently passed less comprehensive laws on privacy than California's CCPA. Illinois, Louisiana, and New Jersey also have limited proposals pending. While legislation in some states may move forward by the end of 2020, states who did not pass a privacy bill convened task forces to study the issue and issue recommendations for next steps. The landscape of state privacy legislation is changing rapidly—the examples stated in this paper may differ as lawmakers continue to weigh on privacy issues.

Whether they are comprehensive bills such as the CCPA or more tailored bills such as Nevada's SB 220, state-by-state privacy legislation will only increase the regulatory burden on credit unions. The following list provides a few examples of state bills on data privacy in various stages of the legislative process:

- ***Illinois: HB 3358.*** Illinois' "Data Transparency and Privacy Act" would create CCPA-like consumer rights to notice, right to know, and opt-out of the sale of their personal data. This bill passed the House but stalled in the Senate after an attempt to add an amendment to provide for class-action enforcement under Illinois consumer class-action statutes.

- ***New Jersey: S2834 and S3497.*** S2834 would require commercial internet websites and online services that collect personally identifiable information from consumers to provide notice of such data collection and disclosures to third parties and allow consumers to opt out. S3497 would require mobile application companies to establish a notice mechanism and require options for consumers if they collect geolocation or GPS data. S2834 is currently under consideration by the Senate Commerce Committee

65 Hunton Andrews Kurth, Alabama Becomes Final State to Enact Data Breach Notification Law, PRIVACY & INFO. SEC. LAW BLOG (Apr. 3, 2018).

66 *See* Mitchelle Noordyke, "US State Comprehensive Privacy Law Comparison," International Association of Privacy Professionals (Apr. 18, 2019).

67 *Id.*

68 Nev. Rev. Stat. Ch. 603A.

and S3497 was referred to the Senate Economic Growth Committee in February 2019. Both bills have identical companion bills in the New Jersey Assembly.

- ***Nevada: SB 220.*** On May 29, 2019, the Governor of Nevada signed SB 220, requiring websites and online services to post a privacy notice and provide consumers with an opportunity to opt out of sale. Provisions regarding breach notification do not apply to entities that are regulated by the GLBA, including credit unions.

- ***Minnesota: HF 2917/SF 2912.*** HF 2917 and SF 2912 would give consumers rights similar to the GDPR including a right to access and transfer their personal data, a right to data deletion and rectification, and the ability to restrict or object to the processing of their data for certain purposes. It would also require breach notifications to consumers. Similar to the CCPA, it contains an exception for data already governed by GLBA, but not organizations regulated by the GLBA.

- ***Puerto Rico: P. del S. 1231.*** The Digital Privacy Protection Act mirrors the CCPA. It would require businesses to notify consumers their personal information may be sold to a third party and are made aware of their rights, including an opt-out-of-sale, should they object to the sale of their data. The bill also creates a private right of action for violations of the bill's provisions. Like the CCPA, the bill contains and exception for information that is regulated by the GLBA.

- ***Washington: SB 5376.*** The Washington Privacy Act, much like the GDPR, would grant consumers the right to know who has obtained their personal data and provided justification for its use, the right to delete certain data and the right to prevent the sale of their data. This bill passed the Senate but stalled in the House after several proposed amendments. The measure has yet to reach the a vote. Senate sponsors of the bill have vowed to reintroduce it in 2020.

One other state effort merits further discussion as it is the most comprehensive bill to date and could move quickly through future legislative sessions.

- ***New York: SB 5642.*** The New York Privacy Act would require businesses to disclose its process of de-identifying personal information, place limitations on sharing consumer information with third parties, allow consumers to learn the names of all entities with whom their personal information is shared, and establish a new Office of Privacy and Data Protection. Although many of these provisions are similar to those of the

CCPA, New York's Privacy Act is significant as it includes a private right of action and establishes a fiduciary duty for businesses to guard consumers' data.

- ***Private Right of Action:*** In addition to granting the Attorney General the power to bring a lawsuit on behalf of a person who has been harmed by a business in violation of the bill's provisions, the bill permits any person who has been injured to sue companies directly over privacy violations. Unlike the CCPA, which applies only to businesses with annual gross revenues over $25 million, the New York Privacy Act applies to all businesses.

- ***"Data Fiduciaries":*** The bill requires companies to act as "data fiduciaries," establishing a fiduciary duty to act in the best interest of the consumer and not use their personal data to benefit solely their companies. Further, the bill prohibits companies from using personal data to cause "unexpected and highly offensive" financial or physical harm to consumers. These duties are required to supersede the other fiduciary duties owed to companies' shareholders.

These provisions, among others, have prompted many to characterize this bill as even more extreme than the CCPA. Unsurprisingly, several tech giants and others have objected to these provisions. The bill did not pass out of the Senate Committee on Consumer Protection before the New York legislative session ended on June 19, 2019, but the legislation (or similar legislation) will likely be reintroduced during the next session.

In the absence of federal action, it is likely that state legislatures will continue to propose study and pass additional privacy laws in the coming years. This patchwork of laws results in an exponentially more burdensome landscape for credit unions compared to a single nation-wide standard. Most of these rules require specific notices and disclosures regarding a credit union's privacy practices; however, these notices requirements often differ from state to state. This could result in confusion for consumers and unnecessary duplicative compliance costs for credit unions.

Further, compliance with new privacy laws requires significant internal structures to support activities such as responding to requests to view the data about a consumer, fielding requests for the deletion of data and tracking consumers' opt-out requests for different kinds of processing and collection. For example, the CCPA regulations as proposed would require that credit unions establish a website plugin to operationalize

the right to opt-out while a consumer browses the website.[69] Other states may require different mechanisms for the opt-out, different language to be used regarding and opt-out, or for a plugin to offer different functionality. Requiring that these kinds of structures be sufficiently flexible to comply with the requirements of multiple jurisdictions is an unreasonable burden for credit unions and unhelpful to consumers. A single, nation-wide privacy standard is necessary for credit unions to provide consistent and useable privacy disclosures and controls to their members.

FEDERAL LEGISLATIVE EFFORTS

With the EU's GDPR already in effect, California's CCPA set to take effect January 1, 2020, other states considering data privacy legislation, and numerous high-profile data breaches sparking consumer outrage, the pressure is on for Congress to consider a comprehensive federal standard. Although there is bipartisan agreement for congressional action, the specifics of such action are unclear. Considering the precedents set by GDPR and CCPA, Congress seems to be leaning toward federal legislation that comprehensively addresses the issue of "data protection," which combines data privacy and data security.[70] Such an approach typically relies on enumerated individual rights in addition to obligations for entities that handle personal information.[71] The specific rights and obligations have been the subject of much congressional debate.[72]

The fact that the US has historically taken a sectoral approach to data privacy further complicates the debate, as questions remain regarding the scope of any federal law. Congress must consider whether legislation should be comprehensive, or perhaps exclude some entities, such as credit unions, that are subject to sector-specific laws (i.e., the GLBA) as some states have already proposed. Various congressional committees are considering the issue from both perspectives, including the House Judiciary, Senate Banking and House Financial Services committees. For example, Chairman Mike Crapo (R-Idaho) and Ranking Member Sherrod Brown (D-Ohio) of the Senate Banking

---

69 California Department of Justice, Notice of Proposed Rulemaking Action, Cal. Code Regs. tit. 11, § 999.315(a).

70 Wilson C. Freeman, Chris D. Linebaugh, & Stephen P. Mulligan, Cong. Research Serv., R45631 *Data Protection Law: An Overview* 54 (2019) (citing ANDREW BURT & ANDREW E. GREER, JR., STANFORD UNIV., HOOVER INST., AEGIS SERIES PAPER NO. 1816, FLAT LIGHT: DATA PROTECTION FOR THE DISORIENTED, FROM POLICY TO PRACTICE 9 (2018) ("What we call 'privacy' and 'security' are now best and jointly described as 'data protection.'"); Woodrow Hartzog & Daniel J. Solove, The Scope and Potential of FTC Data Protection, 83 GEO. WASH. L. REV. 2230, 2232 (2015) (referring to data privacy and security as "two related areas that together we will refer to as 'data protection.'")).

71 *Id.*

72 *Id.* (citing recent hearings before Congress including, Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Commerce, Science, and Transp., 116th Cong. (2019); Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Protection and Commerce of the H. Comm. on Energy and Commerce, 116th Cong. (2019)).

committee solicited public comment on the collection, use and protection of sensitive information and have held several hearings, including "Privacy Rights and Data Collection in a Digital Economy"[73] and "Data Brokers and the Impact on Financial Data Privacy, Credit, Insurance, Employment and Housing."[74]

Another conceptual issue for Congress to consider is whether to use a "prescriptive" or "outcome-based" approach. The GDPR and CCPA rely on a prescriptive approach, defining data protection rules and requiring covered entities to follow these guidelines. Thus far, federal legislative proposals seem to favor the prescriptive approach, as enforcement is more straightforward. However, the Trump Administration, through the U.S. Department of Commerce and the National Telecommunications and Information Administration, has advocated for an outcome-based approach, which evaluates the outcomes of covered entities' practices, rather than prescribing the practices.[75]

There is disagreement as to who should enforce a federal data protection standard. Some lawmakers have proposed the creation of a new federal privacy enforcement agency.[76] Many privacy advocates and industry representatives argue that the likeliest candidate is the Federal Trade Commission (FTC), but with expanded powers and funding. Generally, the FTC has broad authority to bring enforcement actions to protect consumers against unfair or deceptive practices under section 5 of the Federal Trade Commission Act,[77] which prohibits "nfair or deceptive acts or practices in or affecting commerce." Currently, the FTC has GLBA enforcement authority for entities that meet the definition of a "financial institution" but are not subject to the CFPB or do not have a prudential regulator.[78]

However, many entities are not subject to the GLBA and the FTC cannot levy civil financial penalties for first-time UDAP violations[79] making broad enforcement against those engaging in bad privacy practices difficult. Further, the FTC has more extensive

---

73 Privacy Rights and Data Collection in a Digital Economy: Hearing before the S. Comm. On Banking, Housing, and Urban Affairs, 116th Cong. (2019).

74 Data Brokers and the Impact on Financial Data Privacy, Credit, Insurance, Employment and Housing: Hearing before the S. Comm. On Banking, Housing, and Urban Affairs, 116th Cong. (2019).

75 *See* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018) ("The Administration is instead proposing that discussion of consumer privacy in the United States refocus on the outcomes of organizational practices, rather than on dictating what those practices should be.").

76 H.R. 4978, 116th Congress (2019).

77 *See* 15 U.S.C. 41 et seq.

78 15 USC §§ 6809 and 6805.

79 15 U.S.C. § 45(l)–(m) (the FTC generally issues civil penalties only in response to violations of consent decrees or cease and desist orders).

requirements for rulemaking than those under the Administrative Procedure Act (APA) which has led the FTC to rarely use its rulemaking authority.[80] Finally, the FTC has limited resources to dedicate to enforcing a proposed standard, with around 40 staff members to conduct investigations and manage enforcement actions across the country.[81] These supervision and enforcement issues would need to be addressed if the FTC were to enforce a comprehensive federal data protection law.

Moreover, congressional debate continues over preemption, whether a federal regime should expressly preempt state law. Considering the size and strength of the California economy, absent federal action, the CCPA is widely viewed as a *de facto* national law. Industry advocates and members of Congress that dislike the CCPA are eager to pass a federal standard that preempts state law and creates a new national standard. However, House Democrats (of whom 20 percent represent California) are unlikely to accept preemption unless the federal standard is at least as strong as the CCPA, leaving Congress at an impasse.

Overall, Congress seems to agree that some type of action must occur and progress has been made on proposals in both chambers, but no consensus has emerged. Legislative proposals have come from both sides of the aisle, such as the Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act) from Senator Catherine Cortez Masto (D-Nevada)[82] and the American Data Dissemination Act (ADD Act) from Senator Marco Rubio (R-Florida).[83] Several committees are actively engaged in bipartisan efforts; however, considering the myriad points of contention that still must be addressed, it is unlikely that legislation will be enacted this year.

CONSIDERATIONS FOR A FEDERAL DATA PRIVACY STANDARD

The current data privacy landscape has confused businesses and consumers alike. The lack of a federal data privacy law and the rise of patchwork privacy laws presents a burdensome and uncertain environment for credit unions. NAFCU's 2019 Federal Reserve Meeting survey suggests that many credit unions are concerned about the current legal landscape for data privacy. Over 52 percent of respondents stated that they are concerned about the GDPR and 37.1 percent of respondents stated they are concerned

80 *See* 15 U.S.C. § 57a. *See also* Jeffrey S. Lubbers, *It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1989–1990 (2015).

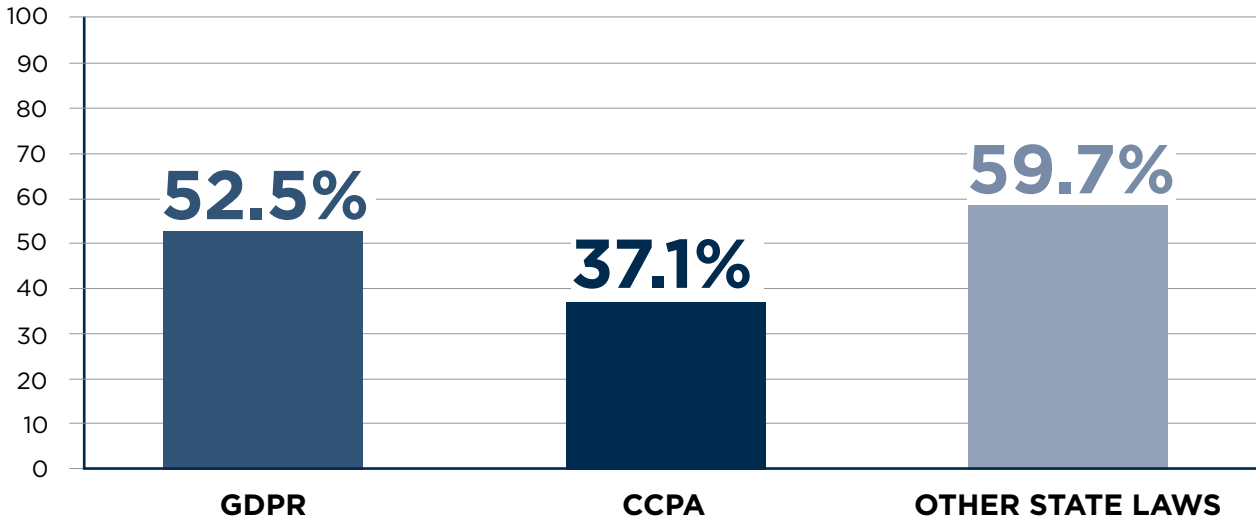
81 Rich, Jessica, "Give the F.T.C. Some Teeth to Guard Our Privacy." The New York Times, Opinion, August 12, 2019.

82 S. 583, 116th Cong. (2019).

83 S. 142, 116th Cong. (2019).

about the CCPA.[84] In particular, credit unions surveyed indicated the highest level of concern, 59.7 percent, for compliance with other state laws as many states consider legislation in this area.[85]

CREDIT UNIONS' LEVEL OF CONCERN REGARDING CURRENT PRIVACY LAWS



Increased data privacy compliance concern is not only a credit union issue; it is a growing issue that affects a variety of institutions of all sizes. Increasingly fragmented privacy laws threaten the ability of businesses, including credit unions, to innovate and grow. Businesses are investing millions of dollars updating their privacy and data security practices to catch up to the newest privacy law.[86] Because of the patchwork legislation, credit unions will be forced to approach privacy regulations on a case-by-case basis. Such a process is unsustainable and presents great risk to credit union industry growth. In particular, the complexities and operational requirements of these laws pose challenges with respect to the significant amount of resources necessary to implement comprehensive compliance programs and the likely difficulty in integrating compliance solutions across multiple systems and services.

Compliance with these laws detracts from a credit unions' ability to efficiently allocate resources to other consumer products and services. The costs of privacy law compliance include conducting significant back-end assessments to understand an institution's risks, building systems and channels for opt-out programs and other requests, and

84 NAFCU 2019 Federal Reserve Meeting Survey.

85 *Id.*

86 *See e.g.*, Nina Trentmann, Companies Worry That Spending on GDPR May Not Be Over, The Wall Street Journal (May 25, 2018).

establishing systems for the creation of meta-data and tracking of personal information. These tasks are likely to include the hiring of consultants, consideration of third-party software solutions and hiring additional staff. Because of the structural and operational implications of these laws, conflicting and changing requirements pose a significant cost and strategic risk to credit unions. Constantly evolving state requirements for data privacy would make it difficult for credit unions to identify whether third-party solutions are worth the long-term investment or to determine the appropriate website and mobile banking platforms protections. For smaller credit unions, more burdensome compliance in the area of privacy would especially hinder their ability to serve members in their respective communities.

The CCPA and other state laws fail to consider the not-for-profit mission and cooperative structure of credit unions. Instead of exempting credit unions from the CCPA because they are already subject to the GLBA, the CCPA and other state laws only provide a small carve-out or impose further regulatory burden on credit unions. Federal legislation on data privacy should recognize that credit unions are already subject to the GLBA and thus should harmonize with the GLBA's requirements so that credit unions can continue to serve as a vital source of credit in their communities. NAFCU supports a comprehensive federal data privacy standard that does not impose upon regulated entities a dual enforcement regime and considers existing statutory requirements regarding the privacy of consumer data.

RULEMAKING AND ENFORCEMENT

In the United States, there is no single statutory authority dedicated to protecting individuals' personal information. There are some federal laws in place to regulate data privacy but these laws are not uniformly applied across sectors.[87] For regulated industries, such as financial institutions, communication providers, and health care entities, the regulatory authority responsible for rulemaking and enforcement depends on the particular law or regulation.

Although some have argued that a comprehensive federal privacy law should delegate privacy rulemaking and enforcement power entirely to the FTC, the delegation of authority regarding a privacy standard to a single agency would be ineffective. For entities without a regulator (such as retailors and fintech), the FTC should be granted rulemaking and

87 *See* Daniel Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUM. L. REV. 583, 587 (2014) ("... Unlike the privacy laws of many industrialized nations, which protect all personal data in an omnibus fashion, privacy law in the United States is sectoral, with different laws regulating different industries and economic sectors...").

enforcement authority. Given the existing shortage of staff working on privacy issues, this will likely require additional resources even without expanding the FTC's jurisdiction over financial institutions. For financial institutions, Congress should follow the GLBA's model to grant rulemaking and enforcement authority to their respective enforcement agencies.

The delegation of responsibility of data privacy enforcement to the primary regulators of the respective industries is not unique; the CFPB, FTC, NCUA, and federal banking agencies share rulemaking and civil enforcement authority for GLBA's privacy provisions. Currently, the FTC and the CFPB share rulemaking authority over the GLBA's Financial Privacy Rule. The GLBA's Safeguards Rule instructs each of the federal banking agencies to establish "appropriate safeguards" for the protection of customer records and information for the financial institutions under their jurisdiction.[88] The CFPB has exclusive enforcement authority over depository institutions, including credit unions with over $10 billion in total assets; federal banking agencies and the NCUA have exclusive enforcement authority over depository institutions and credit unions with $10 billion or less in total assets.[89] The CFPB and FTC share enforcement authority over the remaining non-depository financial institutions covered under the GLBA.[90]

Credit unions are already subject to a multitude of regulations and guidance promulgated by the CFPB, NCUA, the Federal Financial Institutions Examination Council (FFIEC) and examined for compliance with those requirements regularly. Notably, Part 748 is much more comprehensive than the FTC's Safeguards Rule.[91] Currently, the FTC's requirements under the Safeguards Rule lack specific guidelines for safeguard programs or any requirements regarding breach response. The FTC recognizes that the current laws are insufficient and recently proposed to amend its data security rules for financial institutions to "better protect consumers and provide more certainty for business."[92] In contrast, Part 748 of the NCUA provides robust guidelines for safeguard programs, including requirements regarding breach response.[93]

NCUA's familiarity with the credit union industry and the interagency cooperation through the FFIEC has developed a significant understanding of the operations and

88 15 USC §§ 6801(b), 6805(a).
89 *Id. supra note* 42.
90 *Id.*
91 16 CFR §314.4(c).
92 FTC, FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules (March 5, 2019).
93 12 U.S.C. § 748.

activities of financial institutions and the associated risks. This degree of specificity and tailoring is highly valuable to both credit unions and the members they serve. Because of this depth of knowledge, experience and existing frameworks and guidance, it is most practical to grant the NCUA with the rulemaking and enforcement authority under a new privacy framework. The NCUA, the prudential regulator for credit unions, has specialized knowledge of the industry and the required expertise to effectively and efficiently enforce a federal privacy law.

FTC enforcement would still play a critical role in establishing shared responsibility for protecting the sensitive, personal and financial information of American consumers. Unlike credit unions and other depository institutions, which are required to meet certain criteria for protecting consumers' personal information, there is no comprehensive regulatory structure similar to the GLBA that covers non-financial institution entities who collect and hold sensitive information. A national data privacy standard implemented and enforced by the FTC would provide consumers with established expectations for the use of their information and consistent protections across all businesses in the United States. NAFCU strongly supports a federal privacy law that requires any entity responsible for the storage of consumer data to meet similar standards to those imposed on financial institutions, like credit unions.

CONFLICT OF LAWS AND PREEMPTION

One of the most critical reasons for a national privacy standard is the current incongruent interpretation of key terms. As states are moving to pass privacy legislation (with some successfully passing laws), there is an emerging conflict of scope and coverage determinations, definitions, exemptions and private rights of action. For example, the GDPR's definition of personal information is different from that of CCPA's, which is different from almost every other state data breach law. In short, practically every privacy law that is enacted has its own definition of what is protected. Of particular importance are the definitions of *who* is protected and *what* constitutes a data breach.

- ***Data Subject/Consumer:*** Most state data protection statutes typically cover a "consumer" residing in the state. However, the definition of "consumer" differs by state, with some states failing to define "consumer" altogether. The CCPA's current definition is too broad as it defines "consumer" as a "natural person who is a California resident" regardless of the level of involvement of the consumer has with the entity.[94] In contrast,

94 Cal. Civ. Code § 1798.140(g) and Cal. Code Regs. tit. 18, §17014.

the GLBA more narrowly defines "consumer" to mean "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative."[95]

- ***Businesses:*** The state-by-state coverage of who is regulated creates potential conflicts for businesses looking to comply. Hawaii's proposed privacy bill (SB 418) has a broader reach than the CCPA because it does not define "business;" this potentially extends the applicability of the law to all organizations operating in Hawaii. In addition, most state legislation defines businesses as "[a]ny for-profit legal entity"; however, the required criteria, including revenue, varies from state to state.[96]

- ***Consumer Rights (Right to Opt-Out; Access; Deletion):*** The specific rights granted to consumers is also another area where laws are not uniform across state lines. The right to opt-out is inconsistently defined; some state bills have a more expansive requirement than the CCPA, applying to any disclosure of personal information to third parties. For example, New York's privacy bill (SB 5642) includes a broad consumer right to opt-out of any processing, not just the sale of personal information. In addition, not all state bills' access rights include specific information held by the entity or the names of third parties who have received the information. North Dakota (HB 1485) includes a broad prohibition on disclosure of personal information except upon explicit consent. Additionally, some states have a narrow deletion right where they only allow consumers to demand deletion of data they have provided; however, other states like Maryland have an expansive deletion right, allowing consumers to demand deletion of any personal data a covered entity maintains.[97]

Currently, the CCPA and other comprehensive state privacy bills do not take a consistent approach with respect to GLBA-regulated financial institutions.[98] Notably, none of the proposed laws provide a complete carve-out for GLBA-regulated entities. Instead, Maryland, Massachusetts, Puerto Rico and Washington are consistent with the CCPA in providing a carve-out for personal information that is subject to the GLBA but not all personal information held by GLBA-regulated entities. In contrast, the proposed

95 12 C.F.R. § 1016.3(e)(1).
96 *See* Hawaii, S. 418; see also New York, SB 5642.
97 Maryland, S. 0613.
98 See Cal. Civ. Code § 1798.145(e);

legislation in Hawaii, New Jersey, Nevada and Rhode Island does not currently contain any GLBA carve-outs. Although the proposed bills are subject to change, the potential for differing treatment of financial institutions is of particular concern for credit unions who want a clear privacy law when building their privacy compliance programs.

The right of private action also varies across state lines.

- ***Data Breach:*** The CCPA offers a private right of action for data breaches.[99] Currently, due to the lack of a federal data privacy standard, the definition of data breach depends on the individual state statute and typically involves unauthorized access or acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.

- ***Any Violation:*** Some jurisdictions including Massachusetts and Puerto Rico have proposed a private right of action for any violation of this proposed law, not just for breach of data.[100]

- ***No Private Right of Action:*** Some state bills, such as those out of Washington and Hawaii, do not grant a private right of action for any violation of their proposed privacy law nor do they specify any penalties.

The introduction of new state data privacy and security bills across the United States raises major compliance and legal concerns for credit unions operating across state lines. Although many of these laws are still in the approval process, credit unions of all sizes are realizing the enormous effort required to comply with potentially 50 distinct laws and the consequences of violations and/or legal action for alleged non-compliance.

These inconsistent state laws pose a significant logistical problem as individual pieces of data may be subject to different regulatory schemes. The same piece of data may be considered personal data in one jurisdiction, but not in another. A credit union may need to obtain consent to collect that data in one state but may need to offer an opportunity to opt out of that collection in another. In order to ensure that data is appropriate used, credit unions would need systemic capabilities to add metadata to each piece of data so it can reliably track applicable laws for to each piece of data. Credit union systems making

99 Cal. Civ. Code § 1798.150(a)(1).

100 *See* Massachusetts, S.120 and Puerto Rico, P. del S. 1231.

use of that data would then need systemic capabilities to ensure that data is filtered such that it is not used or shared inappropriately. This technology does not currently exist., Because the proposed laws are so different and prescriptive, credit unions would not even have the ability to choose to comply with the most stringent laws as a safe harbor.

These logistical problems not only stifle credit union growth, it may deter credit unions from offering products and services in certain jurisdictions because of the heavy compliance burdens imposed by the state privacy laws. Significantly, smaller credit unions would suffer the most from the costs of compliance with different state regulations. As such, the appropriate solution is a comprehensive federal privacy standard that would harmonize existing privacy laws and preempt all state privacy laws.

CONCLUSION

Now is the time for Congress to pass a comprehensive federal privacy law that protects consumers and preempts piecemeal state privacy laws. A federal law that preempts state privacy laws need not water down privacy standards nor must it provide a one-size-fits-all solution. Rather, Congress should establish a single, comprehensive, principles-based standard that encompasses existing federal privacy standards, such as the GLBA, and grants rulemaking authority to the appropriate sectoral regulator. Credit unions, especially small credit unions, would greatly benefit from a federal privacy standard that takes into consideration their existing compliance obligations and allows them to build a strong compliance program to best protect their members across multiple states. The growing patchwork of state privacy laws would harm businesses and consumers alike. A federal privacy law would not only be more efficient for businesses but also more effective in protecting consumers across our nation. As such, Congress should provide targeted rule-making authority to the NCUA and other sectoral regulators to ensure they can adapt to a rapidly changing landscape. The integrity and safety of our nation's sensitive consumer data depends on building a strong federal data privacy law that covers all players in the market.

APPENDIX: COMPARISON TABLE OF THE CCPA AND GDPR

The following table highlights some of the significant similarities and differences between the CCPA and GDPR. This table is not intended to be a comprehensive or exhaustive review of either the GDPR or the CCPA and credit unions seeking information about either should consult their local attorney. However, this table does illustrate the significant burden posed on credit unions subject to multiple, comprehensive privacy laws in the absence of a single, federal privacy standard.

Topic	CCPA	GDPR	Comparison
Regulated Entities	The CCPA directly impacts businesses that operate in the state of California.[101]	The GDPR affects businesses that offer products or services within the EU or monitor the behavior of individuals in the EU, regardless if the company is physically located in the EU.[102]	The GDPR's scope and jurisdiction is broader because under the GDPR, even if entities are not established in the EU but offer goods and services or monitor the behavior of individuals within the EU, they are subject to the GDPR to the extent they process the personal data of those individuals. The CCPA applies to certain controllers that "do business in the State of California" regardless of where they are located but only to the extent that they process data of California residents.
Covered Individuals	"Consumers" is defined as California residents.[103]	"Data subjects" is defined as identified or identifiable persons to which personal data relates.[104]	The GDPR's definition of "data subjects" is more expansive than CCPA-covered "consumers" but both laws only apply to the data collection of "natural persons" and are not applicable to businesses. GDPR refers to "natural persons" and "data subjects" as covered individuals. The jurisdictional reach of the GDPR depends on whether a product or service is delivered in the EU and personal data is processed and/or monitored as a result.
Covered Information	Personal information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household.[105]	Personal data is any information relating to an identified or identifiable data subject; a lawful justification for processing certain data applies.[106]	The GDPR covers information that identifies a natural person, directly or indirectly (i.e., a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person).[107]

101 Cal. Civ. Code § 1798.140(c).
102 GDPR Art. 3.
103 Cal. Civ. Code § 1798.140(g) and Cal. Code Regs. tit. 18, §17014.
104 GDPR Art. 4(1).
105 Cal. Civ. Code §§ 1798.140(o) and 1798.145(c)-(f).
106 GDPR Art. 4(1) and 9(1).
107 GDPR Art. 4(1).

Topic	CCPA	GDPR	Comparison
Privacy Notice	The CCPA requires that businesses provide specific information to consumers and establishes delivery requirements as well as third party requirements to give consumers explicit notice and an opportunity to opt out before re-selling personal information that the third party acquired from another business.[108]	Data controllers must provide detailed information about its personal data collection and data processing activities. The notice must include specific information depending on whether the data is collected directly from the data subject or a third party.[109]	Both the CCPA and GDPR require detailed privacy notices, however, the required content of those notices differs.
Security Requirements	The CCPA does not require covered entities to have specific data security measures. The CCPA establishes a private right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk arising from existing California law.[110]	The GDPR requires data controllers and data processors to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk.[111]	Both the GDPR and the CCPA require covered entities to have reasonable/appropriate security measures but do not directly impose specific data security requirements.
Opt-Out Right for Personal Information Sale	The CCPA grants individuals an absolute right to opt-out of the sale of their personal information and obligates businesses to add a "Do Not Sell My Personal Information" link on websites and mobile apps.[112]	The GDPR does not grant individuals specific right to opt-out of personal data sales. However, it does permit data subjects, at any time, to object of processing data for marketing purposes and withdraw consent for processing activities.[113]	There is no opt-out requirement under the GDPR. However, the CCPA grants individuals an absolute right to opt-out of the sale of their personal information.

108 Cal. Civ. Code §§ 1798.100(a) - (b), 1798.105(b), 1798.110, 1798.115, 1798.120(b), 1798.130, and 1798.135.
109 GDPR Art. 13-14.
110 Cal. Civ. Code § 1798.150(a)(1).
111 GDPR Art. 24(1) and 32.
112 Cal. Civ. Code § 1798.150(a)(1).
113 GDPR Art. 24(1) and 32.

Topic	CCPA	GDPR	Comparison
Right of Access, Disclosure and Data Portability	Customers have a right to obtain a written disclosure of information. If a customer requests disclosure, a business must provide personal information in a readily useable format to enable a consumer to transmit the information from one entity to another entity without hindrance.[114]	Under the GDPR, data subjects have a broad right of access to information. Data must be provided in a "structured, commonly used and machine-readable format" that can be transferred.[115]	Both laws specify that data controllers/ businesses must have in place mechanisms to verify that the request is made by the consumer/data subject. The CCPA requires a business to disclose a consumer's personal information for a business purpose pursuant to a written contract and the right of access applies only to personal information collected in the 12 months prior to the request.
Right to Deletion/ Erasure	A consumer has the right to deletion of personal information a business has collected, subject to certain exceptions. The business must also instruct its service providers to delete the data.[116]	Data subjects have the right to request erasure of personal data, subject to exceptions. Data controllers must also take reasonable steps to inform other data controllers also processing the data of the request for deletion.[117]	Both the GDPR and the CCPA allow individuals to request the deletion of their personal information, unless exceptions apply. The scope, applicability and exemptions of the right to deletion differ.
Penalties	The California AG may bring actions for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional. The CCPA also establishes a narrow private right of action for certain data breaches involving some personal information. However, the CCPA also grants businesses a 30-day cure period for noticed violations.[118]	The GDPR imposes civil fines and establishes a private right of action for material or non-material damage caused by a data controller or data processors breach of the GDPR.[119]	In addition to civil penalties, both the CCPA and GDPR establish a private right of action.

114 Cal. Civ. Code §§ 1798.100(d) and 1798.130(a)(2).
115 GDPR Art. 20.
116 Cal. Civ. Code § 1798.105.
117 GDPR Art. 17.
118 Cal. Civ. Code § 1798.150 and 1798.155.
119 GDPR Art. 82 and 83-84.