2022 Data Privacy and Security Update

By Eric Rosenkoetter

This article is an excerpt from the Fall 2022 RMAI Insights *magazine (pages 12, 28, 29 and 30), originally published October 3, 2022.*

This has been a dynamic year for data privacy and security legislation and regulation. At the state level, over 50 comprehensive consumer data privacy bills were introduced, though only two succeeded in passage. In addition, three states amended their data breach notification laws, and one state has initiated formal rulemaking.

At the federal level, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule was significantly amended and includes new requirements that should be of interest to many RMAI members. Regarding federal legislation, H.R. 8152, the American Data Privacy and Protection Act, was introduced on June 21, 2022, and represents the most bipartisan effort to date for a national consumer data privacy law.

This article summarizes the state and federal legislative and regulatory highlights with extra emphasis on the amendments to the Safeguards Rule.

State Data Privacy Laws

Utah and Connecticut

On March 24, 2022, Utah Governor Spencer Cox signed into law SB 227, the Utah Consumer Privacy Act, which goes into effect December 31, 2023. Thereafter, on May 10, 2022, Connecticut Governor Ned Lamont signed into law Substitute Senate Bill 6, commonly referred to as the Connecticut Data Privacy Act, which goes into effect July 1, 2023. Thus, Utah and Connecticut became the fourth and fifth states, respectively, to pass comprehensive consumer data privacy laws following California, Virginia, and Colorado.

Importantly, all the laws except California's exempt both entities and data subject to the GLBA, with California limiting the exemption to just data subject to the GLBA.

The chart on the next page compares some of the important aspects of these laws.

State Data Breach Laws

Arizona

Arizona HB 2146 amended existing law by requiring notification be sent to the Director of the Arizona Department of Homeland Security in the event of a security system breach that affects more than 1,000 individuals.

Indiana

Indiana HB 1351 amended existing law with a 45-day deadline for making the notifications and disclosures required after the discovery of a breach.

Maryland

Maryland SB 643 amended existing law by, among other things: 1) expanding the requirement to implement reasonable safeguards from businesses that own or license such information to also those that "maintain" personal information; 2) specifying the information that must be included in a notification to the attorney general; and 3) modifying the timelines for providing notifications under certain circumstances.

State Data Privacy Regulation

California

On July 8, 2022, the California Privacy Protection Agency

[1] https://cppa.ca.gov/regulations/consumer_privacy_act.html

STATE CONSUMER DATA PRIVACY LAWS						
	CALIFORNIA CONSUMER PRIVACY ACT	**CALIFORNIA CONSUMER PRIVACY ACT** *(As Amended by the California Privacy Rights Act)*	**COLORADO PRIVACY ACT**	**CONNECTICUT DATA PRIVACY ACT**	**UTAH CONSUMER PRIVACY ACT**	**VIRGINIA CONSUMER DATA PROTECTION ACT**
EFFECTIVE DATE	1/1/2020	1/1/2023	7/1/2023	7/1/2023	12/31/2023	1/1/2023
THRESHOLDS	**1.** Annual gross revenue in excess of $25,000,000; **2.** Annually buys, receives, sells, or shares, for commercial purposes, the personal information of 50,000 or more consumers, households, or devices; or **3.** Derives 50% or more of annual revenue from selling consumers' personal information.	**1.** Annual gross revenue in excess of $25,000,000; or **2.** Annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or **3.** Derives 50% or more of annual revenue from selling or sharing consumers' personal information.	**1.** Controls or processes the personal data of 100,000 or more consumers per calendar year; or **2.** Derives revenue from the sale of personal data and processes or controls the personal data of 25,000 or more consumers.	**1.** Controls or processes the personal data of at least 100,000 consumers; or **2.** Controls or processes the personal data of at least 25,000 consumers and derives more than 25% of gross revenue from the sale of personal data.	Annual revenue of $25,000,000 or more, and: **1.** Controls or process personal data of 100,000 or more consumers; or **2.** Derives over 50% of gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.	**1.** Controls or processes personal data of at least 100,000 consumers; or **2.** Controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.
RIGHT TO KNOW AND OBTAIN	X	X	X	X	X	X
RIGHT TO CORRECT		X	X	X		X
RIGHT TO DELETE	X	X	X	X	X	X
RIGHT TO OPT OUT/ RESTRICT	X	X	X	X	X	X
GLBA EXEMPTION	Data level	Data level	Data and entity level	Data and entity level	Data and entity level	Data and entity level
CONTRACT REQUIREMENTS		X	X	X	X	X
RISK ASSESSMENTS		If processing presents a significant risk to	If processing presents a heightened risk of harm.	If processing presents a heightened risk of harm.		If processing presents a heightened risk of harm.
PRIVATE RIGHT OF ACTION	For a security breach, $100 to $750 per incident	Expanded to include the breach of a username and				
RIGHT TO CURE	X	Eliminated	X	X	X	X
ENFORCEMENT/ CIVIL PENALTY	No more than $2,500 per violation, or $7,500 for	No more than $2,500 per violation, or $7,500 for	Unfair or deceptive trade practice; up to a	Unfair trade practice; up to $5,000 per willful	Not to exceed $7,500 per violation	Up to $7,500 per violation
RULEMAKING	X	X	X			

issued a Notice of Proposed Rulemaking[1] relating primarily to the changes made to the California Consumer Privacy Act by the California Privacy Rights Act, which goes into effect January 1, 2023. At the time of this writing, the RMAI Data Privacy and Security Working Group is analyzing the proposed rules and preparing comments.

Federal Legislation

American Data Privacy and Protection Act (ADPPA or Act)
The ADPPA, H.R. 8152, was introduced June 21, 2022, and voted out of the House Committee on Energy and Commerce by a vote of 53-2 on July 20, 2022. At the time of this writing, it had not yet reached the House floor. If it progresses to the Senate, it is expected to receive opposition.

The Act would apply, in part, to entities subject to the Federal Trade Commission Act and provide consumers with rights similar to those found in the state laws.

Entities would be considered compliant with the data security provisions of the Act with respect to data that is subject to, and processed in accordance with, the GLBA Safeguards Rule. Similar compliance standing would apply regarding data subject to, and processed in accordance with, the GLBA Privacy Rule, to the extent there are related requirements in the Act.

A violation of the Act would be treated as an Unfair or Deceptive, Abusive Act or Practice (UDAAP) under the FTC Act, and State Attorneys General would also be empowered with enforcement. Beginning two years after the effective date, a private right of action would exist for compensatory damages, injunctive relief, reasonable attorney's fees and litigation costs.

The Act would preempt state data privacy laws that are covered by the Act.

Federal Regulation

GLBA Safeguards Rule Amendments

The GLBA requires the Federal Trade Commission to issue rules setting forth standards to safeguard certain information. The Safeguards Rule, 16 C.F.R. § 314.1, et seq., applies to customer information held by non-banking financial institutions and "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of [that information]."

> **"Of importance to RMAI members subject to the GLBA, the Safeguards Rule now provides specific elements that must be included in an information security program."**

The Safeguards Rule was recently amended with significant changes to how an information security program should be designed, what they must include, and who needs to be in charge. The amendments became effective January 10, 2022, although some of the most important provisions are not operative until December 9, 2022.

Of importance to RMAI members subject to the GLBA, the Safeguards Rule now provides specific elements that must be included in an information security program.

A single "qualified individual" designated to oversee, implement and enforce the information security program. Previously, the program could be coordinated by a designated employee or employees.

An information security program based on a risk assessment. This is a current requirement, as well as the need to periodically perform additional risk assessments. However, effective December 9, 2022, the risk assessment must include:

- Criteria for the evaluation and categorization of identified security risks or threats;
- Criteria for the assessment of the confidentiality, integrity, and availability of information, including the adequacy of the existing controls in the context of the identified risks or threats; and
- Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

Safeguards designed to control identified risks through:

- Access controls, including technical and physical controls, to authenticate and limit access;
- Identification and management of data, personnel, devices, systems, and facilities;
- Encryption of all customer information held or transmitted;
- Secure development practices and security testing for applications used for transmitting, accessing, or storing customer information;
- Multi-factor authentication for any individual accessing any information system;
- Procedures for the secure disposal of customer information no later than two years after the last date the information is used;
- Procedures for change management;
- Policies, procedures, and controls to monitor and log the activity of authorized users and detect unauthorized access, use or tampering.

Regular testing and monitoring of the safeguards' effectiveness. This general requirement is currently in effect, but new requirements effective December 9, 2022, are:

- Annual penetration testing; and
- Vulnerable assessments.

Policies and procedures that include:

- Security awareness training;
- Use of qualified information security personnel to manage risks and oversee the program;
- Security training and updates to address risks; and
- Verification that information security personnel maintain current knowledge of changing information security threats and countermeasures.

Service provider oversight through:

- Selecting service providers capable of maintaining appropriate safeguards, which is a current requirement;
- Requiring the safeguards by contract, which is also a current requirement; and
- Periodically assessing services providers based on the risk they present and the adequacy of their safeguards, effective December 9, 2022.

A written incident response plan, with seven specific requirements, designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information.

A regular written report, prepared at least annually, by the qualified individual to the board of directors that includes the status of, and compliance with the information security program, and any related material matters.

Because the elements are now far more specific, RMAI members subject to the Safeguards Rule should compare these requirements to those of their own programs to ensure compliance by December 9, 2022.

Conclusion

A number of bills this year fell just short of making it to the finish line, and not all were as industry friendly as Virginia, Colorado, Utah and Connecticut. With additional time to explore the pros and cons of existing privacy laws, it is likely the upward trend of state legislation will continue with a greater number of enactments in the absence of a federal law with preemption. RMAI and its Data Privacy and Security Working Group will continue to monitor and respond as necessary to new legislation and regulation and keep members informed of important developments.

Eric Rosenkoetter

Principal

MauriceWutscher

Eric Rosenkoetter is a Principal with Maurice Wutscher LLP and is based in the firm's Austin office. He primarily focuses his practice on regulatory compliance and leads the firm's Audit Section and is a member of the firm's Data Privacy and Security Practice Group. He also directs RMAI's Data Privacy and Security Working Group. Eric earned his law degree from Washington University in St. Louis and his business degree from Southern Methodist University. He is admitted to practice law in Texas and Missouri and all U.S. District Courts in Texas.