OFFICE OF LEGISLATIVE RESEARCH
Objective Research for Connecticut's Legislature
ResearchReport

Encryption of Personal Data by Financial Institutions and Utilities in Connecticut and Neighboring States

By: Matthew Hoppler, Legislative Analyst II
March 5, 2024 | 2024-R-0049

Issue

Do Connecticut and its surrounding states require financial institutions and utility companies to protect a consumer's personal data with encryption?

Summary

Connecticut has several laws that require businesses to protect certain types of personal data that they collect, store, and transmit. The Connecticut Data Privacy Act (CTDPA) requires companies that process a certain amount of consumer personal data employ reasonable cybersecurity practices to prevent unauthorized access or theft. CGA § 42-901(b) provides limited civil liability protection for companies that conform to an industry recognized cybersecurity framework who experience data breaches. Lastly, the Insurance Data Security Law (CGA § 38a-38(c)) requires licensed insurance companies to implement and maintain a comprehensive written information security plan.

Massachusetts requires that persons who own or license a resident's personal data use certain safeguards to protect customer information in a manner fully consistent with industry standards (Mass. Gen. Laws Ch. 93H, § 2). Regulations provide guidance on what safeguards and protections must be in place to comply with the law (201 CMR 17.00).

In 2019, New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) (updating an earlier law). Similar to Massachusetts law, the SHIELD Act requires that any person or business that owns or licenses computerized personal data of a resident develop, implement, and

maintain reasonable safeguards to protect the information. New York also maintains regulations governing the protection of nonpublic information at financial institutions (23 NYCRR 500).

Rhode Island's Identify Theft and Protection Act of 2015 (since amended) (R.I. Gen. Laws § 11-49.3) is similar to both the New York and Massachusetts law on personal data. The law requires persons that store, collect, process, maintain, acquire, use, own, or license personal information about a Rhode Island resident to implement and maintain an information security program.

Below, we provide a broad overview of these laws, focusing on encryption or related requirements.

There is not a comprehensive federal privacy law governing the collection, use, or sale of personal data. Congress has historically addressed personal data privacy and security issues through industry or demographic specific legislation (e.g., the Children's Online Privacy Protection Act of 1998 (P.L. 105-277)). Personal data and customer information at financial institutions is protected by the Gramm-Leach-Bliley Act, which requires federal financial institutions to protect nonpublic customer information (P.L. 106-102). It does not appear there are federal requirements to specifically use encryption to protect consumer data stored by utilities such as electricity and natural gas companies (although more broadly, certain federal requirements for identity theft protection may apply to utilities, including the Federal Trade Commission's (FTC) Red Flags Rule; see the FTC website for related information).

Connecticut

The Connecticut Data Privacy Act (CTDPA), which took effect on July 1, 2023, requires that entities covered under the law protect personal data in its possession. Covered entities include persons conducting business in the state, or that produce products or services targeted to state residents, and that during the prior year processed the personal data of (1) 100,000 or more customers (not including processing just for payment transactions) or (2) 25,000 or more customers and derived 25% or more of their gross revenue from selling personal data. Under the law, a data controller must establish, implement, and maintain reasonable data security practices needed to protect the personal data in its possession. While CTDPA does not explicitly require a covered entity to use encryption to safeguard personal data, using encryption is generally considered a reasonable data practice when storing and transmitting personal data. For more information on the CTDPA, see the attorney general's website.

State law incentivizes Connecticut businesses (specifically, those that access, maintain, communicate, or process personal or restricted information) to create, maintain, and follow a written cybersecurity program with administrative, technical, and physical safeguards for the protection of this information that conforms to an industry-recognized cybersecurity framework

(CGA § 42-901(b)). If they do, the Superior Court is generally prohibited from assessing punitive damages if the business is sued for a data breach. The protection does not apply if the covered entity's failure to implement reasonable cybersecurity controls resulted from gross negligence or willful or wanton conduct. Most current cybersecurity frameworks recommend encrypting all sensitive data when being transmitted or in storage.

The Insurance Data Security Law generally requires licensed insurance companies to develop, implement and maintain a comprehensive written information security program based on a set of risk-based criteria (CGA § 38a-38(c)). As part of its plan, a company must determine if protection, by encryption or other appropriate means, of all nonpublic information while it is transmitted or stored is needed to safeguard personal data (CGA § 38a-38(c)(4)(B)(iv)).

Massachusetts

Massachusetts law required the Department of Consumer Affairs and Business Regulation to adopt data security regulations for persons that own or license a resident's personal data (Mass. Gen. Laws. Ch. 93H, § 2). Those regulations (201 CMR 17.00) require them to encrypt the data when it is being transmitted across public networks or stored on laptops or other portable devices. Further, persons storing personal data on a system connected to the Internet must implement reasonable cybersecurity practices such as employing up-to-date firewalls, virus detection software, and downloading security patches and updates to operating systems (201 CMR § 17.04).

These requirements are part of the more general requirement that people owning or licensing personal information about Massachusetts residents develop, implement, and maintain a comprehensive information security program. The program safeguards must be consistent with the safeguards for protection of personal and similar information in any applicable state or federal regulations. Among other components, the program must also include security policies for employees relating to the storage, access, and transportation of records containing personal data outside of the business premises (201 CMR § 17.03).

New York

New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) requires that any person or business that owns or licenses computerized personal data of a resident develop, implement, and maintain reasonable safeguards to protect the information. To meet this requirement, a person or business must either comply with other specified laws when applicable (e.g., the Gramm-Leach-Bliley Act) or implement a data security program with specified components.

Reasonable safeguards include the ability to detect, prevent, and respond to cyberattacks and system failures as well as physical safeguards to protect against unauthorized access and use of private data. Failure to maintain reasonable safeguards may result in a civil penalty of up to $5,000 per violation.

New York also maintains regulations establishing cybersecurity requirements for financial services companies (23 NYCRR Part 500). The regulations require each covered entity to have a cybersecurity program that uses encryption, in most cases, to protect nonpublic information (such as personal data) either in transit or in storage. If encryption is infeasible, covered entities are permitted to protect nonpublic data using effective alternative means.

Rhode Island

The Rhode Island Identify Theft and Protection Act of 2015 (R.I. Gen. Laws § 11-49.3) requires persons who store, collect, process, maintain, acquire, use, own, or license personal information about a Rhode Island resident to implement and maintain an information security program. The program must include reasonable security procedures and practices to protect personal data.

Violations of the requirements may result in a civil fine of up to $200 depending on the nature of the violation.

Federal Laws and Regulations

Federal law required regulators to establish standards for financial institutions to insure the security and confidentiality of customer records and information (15 U.S.C. § 6801(b)(1)). As such, federal regulations require that financial institutions under the regulatory jurisdiction of the Federal Trade Commission (FTC), such as mortgage brokers and professional tax preparers, maintain a comprehensive information security program (16 C.F.R. § 314.3(a)). As part of this program, the financial institution must protect by encryption all customer information its holds or transmits (16 C.F.R. § 314.4(c)(3)). If for a given reason encryption is practically infeasible, the institution may secure the customer information using effective alternative means that have been approved by a designated person responsible for overseeing the information security program.

MH:kl