MAINE JOINT STANDING COMMITTEE ON JUDICIARY

TESTIMONY OF ERIC ROSENKOETTER IN OPPOSITION TO
LD 1977/HP 1270
An Act to Create the Data Privacy and Protection Act
October 17, 2023

Chairpersons Carney and Moonen and distinguished members of the Committee, my name is Eric Rosenkoetter, and my law firm, Maurice Wutscher LLC, serves as outside counsel to the Receivables Management Association International ("RMAI"). It is an honor to address you this morning.

RMAI is a trade association of over 600 members composed of banks, non-bank lenders, debt buyers, and the companies that support them. These are primarily financial institutions under the Gramm-Leach-Bliley Act ("GLBA").

Respectfully, RMAI opposes LD 1977.

State Data Privacy Landscape

To date, there have been 12 states that have enacted comprehensive consumer data privacy laws,[1] and every state has followed a generally common model. While the laws vary to some degree, the one thing they all share is a GLBA exemption.

Federal Regulation of Financial Institutions

The reason every state has included a GLBA exemption is because financial institutions are already heavily regulated by federal laws that require they protect consumers' information, provide consumers access to their information, and give consumers information and choice about how their information is used.

For example, the GLBA Privacy Rule[2] addresses consumers' privacy rights. The Privacy Rule:

[1] California, Virginia, Colorado, Utah, Connecticut, Iowa, Indiana, Tennessee, Montana, Texas, Oregon, and Delaware.
[2] 16 C.F.R. § 313.1, *et seq.*

- Requires a financial institution to provide notice to customers about its privacy policies and practices;
- Describes when a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and
- Provides a method for consumers to opt out of such sharing.[3]

The GLBA Safeguards Rule,[4] as the name suggests, requires financial institutions to implement safeguards sufficient to protect consumers' personal information. These requirements are too numerous to discuss today, but a summary has been attached to my written testimony. I encourage you to review the attachment.

Additionally, section 1033 of the Dodd-Frank Act[5] requires that financial institutions provide consumers with access to their information relating to financial products or services that have been provided. The Consumer Financial Protection Bureau intends to issue a Notice of Proposed Rulemaking this month.[6]

Burden and Conflict

Financial institutions have developed their compliance management systems around well-established definitions, terms, and requirements that differ from those in LD 1977. Thus, the legislation would create excessive compliance burdens, such as having to constantly map and manage two separate data regimes, and the potential for conflict with other laws which would lead to litigation.

Conclusion

Increased compliance burdens, and litigation associated with conflicts between laws, are costs that would ultimately be passed down and borne by consumers. For this reason, and because of the robust regulatory framework that already exists for financial institutions, RMAI respectfully opposes LD 1977.

Thank you for your time and attention. I can be contacted at 512-672-7068 or erosenkoetter@mauricewutscher.com.

---

[3] 16 C.F.R. § 313.1(a).
[4] 16 C.F.R. § 314.1, *et seq.*
[5] 12 U.S.C. § 5533.
[6] CFPB, Unified Agenda, *Required Rulemaking on Personal Financial Data Rights*; https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=3170-AA78 .

Summary of the Gramm-Leach-Bliley Act Safeguards Rule

The GLBA Safeguards Rule[7] requires financial institutions to protect consumers' nonpublic personal information. In summary, a financial institution is required to:

- Implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue;
- Designate a qualified individual responsible for overseeing, implementing, and enforcing its information security program;
- Base its information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;
- Periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;
- Design and implement safeguards to control the risks identified through risk assessment, including by:
    - Implementing and periodically reviewing access controls, including technical and physical controls;
    - Identifying and managing the data, personnel, devices, systems, and facilities that enable achievement of business purposes in accordance with their relative importance to business objectives and risk strategy;
    - Protecting by encryption all customer information held or transmitted both in transit over external networks and at rest;
    - Adopting secure development practices for in-house developed applications utilized for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;
    - Implementing multi-factor authentication for any individual accessing any information system, unless the Qualified Individual has approved

[7] 16 C.F.R. § 314.1, *et seq.*

in writing the use of reasonably equivalent or more secure access controls;
    - Developing, implementing, and maintaining procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, subject to certain exceptions;
- Periodically review the data retention policy to minimize the unnecessary retention of data;
- Adopt procedures for change management;
- Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users;
- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems;
- Implement policies and procedures to ensure that personnel are able to enact your information security program;
- Oversee service providers, by:
    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
    - Requiring service providers by contract to implement and maintain such safeguards; and
    - Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.
- Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control;
- Require the Qualified Individual to report in writing, regularly and at least annually, to the board of directors or equivalent governing body.