Attachment #24

Rhode Island Bankers Association, 3/26/19 letter

RIBA
RHODE ISLAND BANKERS ASSOCIATION

March 26, 2019

The Honorable Evan P. Shanley
Chair, RI Online Data Transparency and
Privacy Protection Commission
State House
Providence, RI 02903

Re: Proposed Privacy Legislation

Dear Chairman Shanley:

As legislative counsel to the Rhode Island Bankers Association (RIBA), we are asking the RI Online Data Transparency and Privacy Protection Commission to consider an amendment to any proposed legislation ultimately supported by the Commission. The amendment is the same as proposed in your legislation of 2018 – RI Right-To-Know Data Transparency and Privacy Protection Act (H-7111A/3) and would exempt from the provisions of the legislation, those entities subject to the Federal Gramm-Leach-Bliley Act (GLBA). The proposed language would read as follows:

"Nothing in this chapter shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the Federal Gramm- Leach-Bliley Act of 1999 and the rules promulgated under that act."

The Gramm-Leach-Bliley Act (GLBA), enacted by Congress in 1999, required financial regulators to develop strong protections for the security of consumer financial information. The GLBA functional regulators (e.g., the federal banking agencies), imposed wide-ranging information security guidelines for institutions they regulate, pursuant to that Federal law. The banking agencies imposed the most stringent requirements, mandating strong internal security procedures, investigatory requirements for potential breaches, and broad-based notice requirements for breaches where consumers face a real risk of harm.

GLBA has already put in place a robust data protection, consumer notification and examination and enforcement system; and therefore financial institutions subject to these existing standards should not be subject to overlapping and potentially inconsistent requirements in new federal or state legislation.

Overview

Section 501(b) of the GLBA required the banking agencies to establish standards for the banks and other financial institutions subject to their jurisdiction ("financial institutions") to protect the security of customer information. Accordingly, the Agencies issued guidelines requiring financial institutions to implement comprehensive, risk-based information security programs that include administrative, technical and physical safeguards to protect customer information. See, e.g., 12 C.F.R.

pt. 364, App. B (FDIC); 12 C.F.R. pt. 208, App. D-2 and part 225, app. F (FRB); and 12 C.F.R. pt. 30, App. B (OCC).

These guidelines require financial institutions to conduct thorough assessments of the security risks to customer information and customer information systems. Moreover, if a financial institution identifies a risk, the financial institution must adopt an appropriate control to protect against the risk. A financial institution also must take steps by contract and through monitoring to oversee its service providers with access to customer information to ensure that such information is protected. As discussed below, a prominent requirement is that financial institutions maintain programs to respond to unauthorized access to customer information. Moreover, the banking agencies regularly examine financial institutions for their compliance with these requirements.

Response to Data Breach

Financial institutions must implement a "risk-based" response program to address instances of unauthorized access to customer information systems. At a minimum, a response program must:

- Assess the nature and scope of any security incident and identify what customer information systems and customer information may have been accessed or misused.
- Notify the institution's primary federal regulator "as soon as possible" about any threats "to sensitive customer information."
- Notify appropriate law enforcement authorities and file Suspicious Activity Reports in situations involving federal criminal violations requiring immediate attention.
- Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information.
- Notify customers "as soon as possible" if the institution determines that misuse of customer information has occurred or is reasonably possible.

Customer Notice

A critical component of the GLBA guidelines is customer notification. When a financial institution becomes aware of a breach of "sensitive customer information," it must conduct a reasonable investigation to determine whether the information has been or will be misused. If it determines that misuse of the information "has occurred or is reasonably possible," it must notify affected customers "as soon as possible."

Sensitive customer information means the customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, credit card, debit card or other account number or personal identification number or password to access an account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password.

A financial institution must provide a clear and conspicuous notice to consumers. The notice must describe the incident in general terms and the type of customer information affected. It must also generally describe the institution's actions to protect the information from further unauthorized access

and include a telephone number. The notice also must remind customers to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution. Where appropriate, the notice also must include:

- Recommendation to review account statements immediately and report suspicious activity;
- Description of fraud alerts and how to place them;
- Recommendation that the customer periodically obtain credit reports and have fraudulent information removed;
- Explanation of how to receive a free credit report; and
- Information about the FTC's identity theft guidance for consumers.

Penalties for Non-Compliance

Financial institutions are examined on a regular basis by the banking agencies for compliance with the GLBA data protection and consumer notice requirements. Financial institutions that are found not to be in compliance are required to fix identified problems and come into compliance and are subject to various remedies, including monetary penalties and public cease and desist orders.

We remain available to discuss this issue further.

Very truly yours,

RHODE ISLAND BANKERS ASSOCIATION

William A. Farrell

Cc: Danica A. Iacoi, Chief Legal Counsel