2025 -- H 5415 SUBSTITUTE A

========
LC001270/SUB A
========

S T A T E O F R H O D E I S L A N D

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2025

A N A C T

RELATING TO FINANCIAL INSTITUTIONS -- LICENSED ACTIVITIES

Introduced By: Representatives Kennedy, Solomon, Kazarian, Azzinaro, and Ackerman

Date Introduced: February 12, 2025

Referred To: House Corporations

(Dept. of Business Regulation)

It is enacted by the General Assembly as follows:

SECTION 1. Chapter 19-14 of the General Laws entitled "Licensed Activities" is hereby amended by adding thereto the following sections:

19-14-35. Information security program..

(a) Each licensee shall develop, 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 licensee's size and complexity, the nature and scope of activities, including its use of third-party service providers, and the sensitivity of any customer information used by the licensee or is in the licensee's possession.

(b) As used in this chapter, the following terms shall have the following meanings:

(1) "Customer" means a consumer who has a customer relationship with a licensee.

(2) "Customer information" means any record containing nonpublic personal information about a consumer that a licensee has a relationship with, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of a licensee or its affiliates.

(3) "Encryption" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

(4) "Information security program" means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of or

otherwise handle customer information.

(5) "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system such as industrial or process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

(6) "Notification event" means acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Customer information is considered unencrypted for this purpose if the encryption key was accessed by an unauthorized person. Unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless reliable evidence exists that proves there has not been, or could not reasonably have been, unauthorized acquisition of such information.

(7) "Security event" means an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system, or customer information held in physical form, commonly known as a "cybersecurity event".

(c) In order to develop, implement, and maintain the information security program, the licensee shall:

(1) Designate a qualified individual responsible for overseeing, implementing, and enforcing the information security program. The qualified individual may be employed by the licensee, an affiliate, or a service provider. To the extent the requirement in subsection (a) of this section is met using a service provider or an affiliate, the licensee shall:

(i) Retain responsibility for compliance with this section;

(ii) Designate a senior member of the licensee responsible for direction and oversight of the qualified individual; and

(iii) Require the service provider or affiliate to maintain an information security program that protects the licensee in accordance with the requirements of this section.

(2) Perform a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

(i) The risk assessment shall be written and shall include:

(A) Criteria for the evaluation and categorization of identified security risks or threats;

(B) Criteria for the assessment of the confidentiality, integrity, and availability of

information systems and customer information, including the adequacy of the existing controls in the context of identified risks or threats; and

(C) 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.

(ii) A licensee shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

(3) Design and implement safeguards to control the risks identified through risk assessment by:

(i) Implementing and periodically reviewing access controls, including technical and as appropriate, physical controls to:

(A) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(B) Limit authorized users' access only to customer information that they need to perform their duties and functions, or in the case of customers, to access their own information;

(ii) Identify and manage the data, personnel, devices, systems, and facilities that enable the licensee to achieve business purposes in accordance with relative importance to business objectives and the licensee's risk strategy;

(iii) Protect by encryption all customer information held or transmitted both in transit over external networks and at rest. To the extent it is determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, licensee may instead secure such customer information using effective alternative compensating controls reviewed and approved by the qualified individual;

(iv) Adopt secure development practices for in-house developed applications utilized by the licensee for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications utilized to transmit, access, or store customer information;

(v) Implement multi-factor authentication for any individual accessing any information system, unless the qualified individual has approved in writing the use of reasonably equivalent or more secure access controls;

(vi) Record retention:

(A) Develop, implement, and maintain procedures for the secure disposal of customer

information in any format no later than two (2) years after the last date the information is used in connection with the provision of a product or service to the customer which relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and

(B) Periodically review data retention policies to minimize the unnecessary retention of data;

(vii) Adopt procedures for change management; and

(viii) 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.

(4) Based on its risk assessment, the licensee shall perform ongoing testing by:

(i) Regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems;

(ii) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, the licensee shall conduct:

(A) Annual penetration testing of its information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(B) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in the licensee's information systems based on the risk assessment, at least every six (6) months; and whenever there are material changes to operations or business arrangements; and whenever there are circumstances that the licensee knows or has reason to know may have a material impact on the information security program.

(5) Implement policies and procedures to ensure that personnel have the ability to enact the information security program by:

(i) Providing personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(ii) Utilizing qualified information security personnel employed by the licensee or an affiliate or service provider sufficient to manage information security risks and to perform or oversee the information security program;

(iii) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(iv) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(6) Monitor service providers by:

(i) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

(ii) Requiring service providers by contract to implement and maintain such safeguards; and

(iii) Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.

(7) Evaluate and adjust the information security program considering the results of the testing and monitoring required by subsection (c)(4) of this section; any material changes to the licensee's operations or business arrangements; the results of risk assessments performed under subsection (c)(2)(ii) of this section; or any other circumstances that the licensee knows or has reason to know may have a material impact on the information security program.

(8) 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. Such incident response plan shall address the following areas:

(i) The goals of the incident response plan;

(ii) The internal processes for responding to a security event;

(iii) The definition of clear roles, responsibilities and levels of decision-making authority;

(iv) External and internal communications and information sharing;

(v) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(vi) Documentation and reporting regarding security events and related incident response activities; and

(vii) The evaluation and revision as necessary of the incident response plan following a security event.

(9) Require the qualified individual to report in writing, at least annually, to the board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for the information security program. The report shall include the following information:

(i) The overall status of the information security program and compliance with this chapter and associated rules; and

(ii) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

(10) Establish a written plan addressing business continuity and disaster recovery.

(d) The provisions of this section shall not apply to any regulated institution as defined in § 19-1-1, or subsidiary of such regulated institution, or any bank holding company or subsidiary of a bank holding company subject to federal bank holding company laws and regulations.

SECTION 2. Chapter 19-14 of the General Laws entitled "Licensed Activities" is hereby amended by adding thereto the following section:

19-14-36. Notification of a security event.

(a) Each licensee shall notify the director or the director's designee as promptly as possible, but in no event later than three (3) business days from a determination that a security event has occurred when either of the following criteria has been met:

(1) A security event impacting the licensee of which notice is required to be provided to any governmental body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law; or

(2) A security event that has a reasonable likelihood of materially harming;

(i) Any consumer residing in this state; or

(ii) Any material part of the normal operation(s) of the licensee.

(b) The licensee shall provide any information required by this section in electronic form as directed by the director or the director's designee. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the director or the director's designee concerning the security event. The following information shall be provided:

(1) The name and contact information of the reporting licensee;

(2) A description of the types of information that were involved in the notification event;

(3) If the information is possible to determine, the date or date range of the notification event;

(4) The total number of consumers in this state affected or potentially affected by the notification event. The licensee shall provide the best estimate in the initial report to the director or the director's designee and update this estimate with each subsequent report;

(5) A general description of the notification event including how the information was

exposed, lost, stolen, or breached, detailing specific roles and responsibilities of third-party service providers, if any;

(6) A description of efforts being undertaken to remediate the situation that permitted the security event to occur; and

(7) Whether any law enforcement official has provided the licensee with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the director or the director's designee to contact the law enforcement official. A law enforcement official may request an initial delay of up to thirty (30) days following the date when notice was provided to the director or the director's designee. The delay may be extended for an additional period of up to sixty (60) days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the director or the director's designee determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

(8) Name of contact person who is both familiar with the security event and is authorized to act for the licensee.

(c) A licensee shall comply with chapter 49.3 of title 11, as applicable, and provide a copy of the notice sent to consumers under that chapter to the director or the director's designee, when a licensee is required to notify the director or the director's designee.

(d) The provisions of this section shall not apply to any regulated institution as defined in § 19-1-1, or subsidiary of such regulated institution, or any bank holding company or subsidiary of a bank holding company subject to federal bank holding company laws and regulations.

SECTION 3. This act shall take effect upon passage.

========
LC001270/SUB A
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO FINANCIAL INSTITUTIONS -- LICENSED ACTIVITIES

***

This act would provide standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information held by entities licensed under chapter 14 of title 19 relating to licensed activities of financial institutions.

This act would take effect upon passage.

========
LC001270/SUB A
========