HB2829

LRB10110631JLS55737b

101ST GENERAL ASSEMBLY

State of Illinois

2019 and 2020

HB2829

by Rep. Anne Stava-Murray

SYNOPSIS AS INTRODUCED:

New Act

Creates the Financial Institution Cybersecurity Act. Provides that persons and entities operating under the authority of the Secretary of Financial and Professional Regulation under the Illinois Banking Act, the Illinois Insurance Code, the Savings Bank Act, the Illinois Credit Union Act, the Corporate Fiduciary Act, and the Residential Mortgage License Act of 1987 must maintain a cybersecurity program to protect the confidentiality of their information systems. Requires the implementation and maintenance of written policies to protect information systems. Makes provisions for testing, risk assessment, audit trails, and third-party service provider policies. Provides for supervision by the Secretary of Financial and Professional Regulation. Requires annual certifications beginning November 1, 2020. Effective January 1, 2020.

LRB101 10631 JLS 55737 b

FISCAL NOTE ACT
MAY APPLY

A BILL FOR

AN ACT concerning regulation.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Financial Institution Cybersecurity Act.

Section 5. Definitions. In this Act:

(a) "Affiliate" means any person that controls, is controlled by or is under common control with another person. For purposes of this definition, "control" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise.

(b) "Authorized user" means any employee, contractor, agent or other person that participates in the business operations of a covered entity and is authorized to access and use any information systems and data of the covered entity.

(c) "Covered entity" means any person operating under or required to operate under the Illinois Banking Act, the Illinois Insurance Code, the Savings Bank Act, the Illinois Credit Union Act, the Corporate Fiduciary Act, and the Residential Mortgage License Act of 1987.

(d) "Cybersecurity event" means any act or attempt,

successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.

(e) "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 control systems.

(f) "Multi-factor authentication" means authentication through verification of at least 2 of the following types of authentication factors:

(1) knowledge factors, such as a password; or

(2) possession factors, such as a token or text message on a mobile phone; or

(3) inherence factors, such as a biometric characteristic.

(g) "Nonpublic information" means all electronic information that is not publicly available information and is:

(1) business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity;

(2) any information concerning an individual which

because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

(h) "Penetration testing" means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside the covered entity's information systems.

(i) "Person" means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency, or association.

(j) "Publicly available information" means any information

that a covered entity has a reasonable basis to believe is lawfully made available to the general public from: federal, State, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, State, or local law.

For the purposes of this subsection, a covered entity has a reasonable basis to believe that information is lawfully made available to the general public if the covered entity has taken steps to determine:

(1) that the information is of the type that is available to the general public; and

(2) whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) "Risk assessment" means the risk assessment that each covered entity is required to conduct under Section 45 of this Act.

(l) "Risk-based authentication" means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a person and requires additional verification of the person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) "Secretary" means the Secretary of Financial and Professional Regulation.

(n) "Senior officer" means the senior individual or

individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance or risk of a covered entity, including a branch or agency of a foreign banking organization subject to this Act.

(o) "Third-party service provider" means a person that (i) is not an affiliate of the covered entity, (ii) provides services to the covered entity, and (iii) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity.

Section 10. Cybersecurity program.

(a) Each covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems.

(b) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems, and the nonpublic information stored on those information systems, from

unauthorized access, use or other malicious acts;

(3) detect cybersecurity events;

(4) respond to identified or detected cybersecurity events to mitigate any negative effects;

(5) recover from cybersecurity events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A covered entity may meet the requirements of this Act by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this Act, as applicable to the covered entity.

(d) All documentation and information relevant to the covered entity's cybersecurity program shall be made available to the superintendent upon request.

Section 15. Cybersecurity policy. Each covered entity shall implement and maintain a written policy or policies, approved by a senior officer or the covered entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the covered entity's policies and procedures for the protection of its information systems and nonpublic information stored on those information systems. The cybersecurity policy shall be based on the covered entity's risk assessment and address the following areas to the extent

applicable to the covered entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and third-party service provider management;

(m) risk assessment; and

(n) incident response.

Section 20. Chief information security officer.

(a) Chief information security officer. Each covered entity shall designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Act, "chief information security officer"). The chief information security officer may be employed by the covered entity, one of its affiliates or a third-party service

provider. To the extent this requirement is met using a third-party service provider or an affiliate, the covered entity shall:

(1) retain responsibility for compliance with this Act;

(2) designate a senior member of the covered entity's personnel responsible for direction and oversight of the third-party service provider; and

(3) require the third-party service provider to maintain a cybersecurity program that protects the covered entity in accordance with the requirements of this Act.

(b) Report. The chief information security officer of each covered entity shall report in writing at least annually to the covered entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, the report shall be timely presented to a senior officer of the covered entity responsible for the covered entity's cybersecurity program. The chief information security officer shall report on the covered entity's cybersecurity program and material cybersecurity risks. The chief information security officer shall consider to the extent applicable:

(1) the confidentiality of nonpublic information and the integrity and security of the covered entity's information systems;

(2) the covered entity's cybersecurity policies and

procedures;

(3) material cybersecurity risks to the covered entity;

(4) overall effectiveness of the covered entity's cybersecurity program; and

(5) material cybersecurity events involving the covered entity during the time period addressed by the report.

Section 25. Penetration testing and vulnerability assessments. The cybersecurity program for each covered entity shall include monitoring and testing, developed in accordance with the covered entity's risk assessment, designed to assess the effectiveness of the covered entity's cybersecurity program. 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 or indicate vulnerabilities, covered entities shall conduct:

(a) annual penetration testing of the covered entity's information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of information systems reasonably

designed to identify publicly known cybersecurity vulnerabilities in the covered entity's information systems based on the risk assessment.

Section 30. Audit trail.

(a) Each covered entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the covered entity; and

(2) include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity.

(b) Each covered entity shall maintain records required by paragraph(1) of subsection (a) for not fewer than 5 years and shall maintain records required by paragraph (2) of subsection (a) for not fewer than 3 years.

Section 35. Access privileges. As part of its cybersecurity program, based on the covered entity's risk assessment each covered entity shall limit user access privileges to information systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 40. Application security.

(a) Each covered entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the covered entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the covered entity within the context of the covered entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the chief information security officer (or a qualified designee) of the covered entity.

Section 45. Risk assessment.

(a) Each covered entity shall conduct a periodic Risk Assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program as required by this Act. Such risk assessment shall be updated as reasonably necessary to address changes to the covered entity's information systems, nonpublic information or business operations. The covered entity's risk assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the covered entity's business operations

related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems.

(b) The risk assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the covered entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's information systems and nonpublic information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

Section 50. Cybersecurity personnel and intelligence.

(a) In addition to the requirements set forth in subsection (a) of Section 20, each covered entity shall:

(1) utilize qualified cybersecurity personnel of the covered entity, an affiliate or a third-party service provider sufficient to manage the covered entity's cybersecurity risks and to perform or oversee the

performance of the core cybersecurity functions specified in subsection (b) of Section 10 of this Act;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A covered entity may choose to utilize an affiliate or qualified third-party service provider to assist in complying with the requirements set forth in this Act, subject to the requirements set forth in Section 55 of this Act.

Section 55. Third-party service provider security policy.

(a) A covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. Such policies and procedures shall be based on the risk assessment of the covered entity and shall address to the extent applicable:

(1) the identification and risk assessment of third-party service providers;

(2) minimum cybersecurity practices required to be met by such third-party service providers in order for them to do business with the covered entity;

(3) due diligence processes used to evaluate the

adequacy of cybersecurity practices of such third-party service providers; and

(4) periodic assessment of such third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and contractual protections relating to third-party service providers including to the extent applicable guidelines addressing:

(1) the third-party service provider's policies and procedures for access controls, including its use of multi-factor authentication as required by Section 60 of this Act, to limit access to relevant information systems and nonpublic information;

(2) the third-party service provider's policies and procedures for use of encryption as required by Section 75 of this Act to protect nonpublic information in transit and at rest;

(3) notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or the covered entity's nonpublic information being held by the third-party service provider; and

(4) representations and warranties addressing the third-party service provider's cybersecurity policies and procedures that relate to the security of the covered

entity's information systems or nonpublic information.

(c) An agent, employee, representative or designee of a covered entity who is itself a covered entity need not develop its own third-party information security policy pursuant to this Section if the agent, employee, representative or designee follows the policy of the covered entity that is required to comply with this Act.

Section 60. Multi-factor authentication.

(a) Based on its risk assessment, each covered entity shall use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to nonpublic information or information systems.

(b) Multi-factor authentication shall be utilized for any individual accessing the covered entity's internal networks from an external network, unless the covered entity's chief information security officer has approved in writing the use of reasonably equivalent or more secure access controls.

Section 65. Limitations on data retention. As part of its cybersecurity program, each covered entity shall include policies and procedures for the secure disposal on a periodic basis of any nonpublic information identified in paragraphs (2) and (3) of subsection (g) of Section 5 that is no longer necessary for business operations or for other legitimate

business purposes of the covered entity, except where such information is otherwise required to be retained by law or rule, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 70. Training and monitoring. As part of its cybersecurity program, each covered entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such authorized users; and

(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the covered entity in its risk assessment.

Section 75. Encryption of nonpublic information.

(a) As part of its cybersecurity program, based on its risk assessment, each covered entity shall implement controls, including encryption, to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest.

(1) To the extent a covered entity determines that encryption of nonpublic information in transit over external networks is infeasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by

the covered entity's chief information security officer.

(2) To the extent a covered entity determines that encryption of nonpublic information at rest is infeasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the covered entity's chief information security officer.

(b) To the extent that a covered entity is utilizing compensating controls under subsection (a), the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the chief information security officer at least annually.

Section 80. Incident response plan.

(a) As part of its cybersecurity program, each covered entity shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entity's business or operations.

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

(1) the internal processes for responding to a cybersecurity event;

(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

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

(6) documentation and reporting regarding cybersecurity events and related incident response activities; and

(7) the evaluation and revision as necessary of the incident response plan following a cybersecurity event.

Section 85. Notices to Secretary.

(a) Notice of cybersecurity event. A covered entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred that is either of the following:

(1) cybersecurity events impacting the covered entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity.

(b) Annually each covered entity shall submit to the Secretary a written statement covering the prior calendar year. This statement shall be submitted by February 15 in the form required by the Secretary, certifying that the covered entity is in compliance with the requirements in this Act. A covered entity shall maintain for examination by the Secretary all records, schedules and data supporting this certificate for a period of 5 years. To the extent a covered entity has identified areas, systems or processes that require material improvement, updating or redesign, the covered entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Secretary.

Section 90. Confidentiality. Information provided by a covered entity pursuant to this Act is subject to exemptions from disclosure provided under the Illinois Banking Act and the Illinois Insurance Code, the Savings Bank Act, the Illinois Credit Union Act, the Corporate Fiduciary Act, and the Residential Mortgage License Act of 1987.

Section 95. Exemptions.

(a) A covered entity with:

(1) fewer than 10 employees, including any independent contractors, of the covered entity or its affiliates

located in Illinois or responsible for business of the covered entity; or

(2) less than $5,000,000 in gross annual revenue in each of the last 3 fiscal years from Illinois business operations of the covered entity and its affiliates; or

(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates, shall be exempt from the requirements of Sections 20, 25, 30, 40, 50, 60, 70, 75, and 80 of this Act.

(b) An employee, agent, representative, or designee of a covered entity, who is itself a covered entity, is exempt from this Act and need not develop its own cybersecurity program to the extent that the employee, agent, representative, or designee is covered by the cybersecurity program of the covered entity.

(c) A covered entity that does not directly or indirectly operate, maintain, utilize or control any information systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess nonpublic information shall be exempt from the requirements of Sections 10, 15, 20, 25, 30, 35, 40, 50, 60, 70, 75, and 80 of this Act.

(d) A covered entity under Article VIIC of the Illinois Insurance Code that does not and is not required to directly or indirectly control, own, access, generate, receive or possess

nonpublic information other than information relating to its corporate parent company (or affiliates) shall be exempt from the requirements of Sections 10, 15, 20, 25, 30, 35, 40, 50, 60, 70, 75, and 80 of this Act.

(e) A covered entity that qualifies for any of the exemptions pursuant to this Section shall file a notice of exemption in the form set forth as required by the Secretary within 30 days of the determination that the covered entity is exempt.

(f) If a covered entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such covered entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Act.

Section 100. Enforcement. This Act shall be enforced by the Secretary pursuant to the Secretary's authority under this Act and any applicable laws administered by the Secretary.

Section 105. Transitional periods.

(a) Transitional period. Covered entities shall have 180 days from the effective date of this Act to comply with the requirements set forth in this Act, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered entities shall have:

(1) One year from the effective date of this Act to

comply with the requirements of subsection (b) of Section 20, Sections 25, 45, 60, and subsection (b) of Section 70.

(2) Eighteen months from the effective date of this Act to comply with the requirements of Sections 30, 40, 65, subsection (a) of Section 70, and Section 75 of this Act.

(3) Two years from the effective date of this Act to comply with the requirements of Section 55 of this Act.

Section 110. Annual filing. A covered entity shall annually prepare and submit to the Secretary a certification of compliance with this Act under subsection (b) of Section 85 beginning November 1, 2020.

Section 115. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.

Section 999. Effective date. This Act takes effect January 1, 2020.