SB3204

LRB10020137XWW35421b

100TH GENERAL ASSEMBLY

State of Illinois

2017 and 2018

SB3204

Introduced 2/15/2018, by Sen. Michael E. Hastings

SYNOPSIS AS INTRODUCED:

New Act

Creates the Consumer Credit Reporting Agency Registration and Cybersecurity Program Act. Provides for requirements for consumer credit reporting agency registration. Contains provisions regarding grounds for revocation and suspension of a registration. Provides that by January 1, 2019, a consumer credit reporting agency must have a cybersecurity program documented in writing and designed to protect the confidentiality, integrity and availability of its information systems. Provides that a consumer credit reporting agency shall implement and maintain a written cybersecurity policy setting forth its policies and procedures for the protection of its information systems and nonpublic information stored on those information systems. Provides that a consumer credit reporting agency shall designated a qualified individual as a chief information security officer to oversee and implement its cybersecurity policy. Contains provisions concerning penetration testing and vulnerability assessments, audit trail, access privileges, and application security. Provides that a consumer credit reporting agency shall conduct periodic risk assessments of its information systems. Provides requirements for cybersecurity personnel and third-party service provider security policy. Provides that a consumer credit reporting agency shall establish a written incident response plan designed to promptly respond to a cybersecurity event. Provides that the consumer credit reporting agency shall notify the Department of Financial and Professional Regulation of the existence of a cybersecurity event no later than 72 hours after the event occurred. Makes other changes. Effective immediately.

LRB100 20137 XWW 35421 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 Consumer Credit Reporting Agency Registration and Cybersecurity Program Act.

Section 5. Definitions. As used in this Act:

"Affiliate" means a person that controls, is controlled by, or is under common control with another person.

"Authorized user" means any employee, contractor, agent or other person that participates in the business operations of a consumer credit reporting agency and is authorized to access and use any information system and data of the consumer credit reporting agency.

"Consumer" means an individual.

"Consumer report" means a written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal,

family, or household purposes, (ii) employment purposes, or (iii) other purposes.

"Consumer reporting agency" means any person who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports or investigative consumer reports to third parties.

"Consumer credit reporting agency" means a consumer reporting agency that regularly engages in the practice of assembling or evaluating and maintaining public record information or credit account information from persons who furnish that information regularly and in the ordinary course of business for the purpose of furnishing consumer credit reports to third parties bearing on a consumer's credit worthiness, credit standing, and credit capacity.

"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.

"Department" means the Department of Financial and Professional Responsibility.

"Financial institution" means a bank, savings bank, savings and loan association, credit union, or any licensee under the Consumer Installment Loan Act or the Sales Finance Agency Act.

"Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, or any specialized system such as industrial or process control systems, telephone switching and private branch exchange systems, and environmental control systems.

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

(1) knowledge factor, such as a password;

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

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

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

(1) business-related information of a consumer credit reporting agency in which the tampering, or unauthorized disclosure, access, or use of, would cause a material adverse impact on the business, operations or security of the consumer credit reporting agency;

(2) any information concerning an individual that 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) driver's 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 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.

"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 consumer credit reporting agency's information systems.

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

"Publicly available information" means any information that a consumer credit reporting agency 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.

(1) For the purposes of this Act, a consumer credit reporting agency has a reasonable basis to believe that information is lawfully made available to the general public if the consumer credit reporting agency has taken steps to determine:

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

(ii) whether an individual can direct that information to make it unavailable to the general public and, if so, that such individual has not done so.

"Risk assessment" means the risk assessment that each consumer credit reporting agency is required to conduct under Section 65 of this Act.

"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.

"Senior officer" or "senior officers" 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 consumer credit reporting agency, including a branch or agency of a foreign banking organization subject to this Act.

"Third-party service provider" means a person that:

(1) is not an affiliate of the consumer credit reporting agency;

(2) provides services to the consumer credit reporting agency; and

(3) maintains, processes, or otherwise is permitted access to nonpublic information through provision of services to the consumer credit reporting agency.

Section 10. Registration.

(a) A consumer credit reporting agency that assembles, evaluates, or maintains a consumer credit report on one or more consumers located in the State of Illinois shall register with the Department in a form and manner acceptable to the Department.

(b) For a business entity, the officer or officers and director or directors named in the registration application shall be designated responsible for the business entity's compliance with the financial services, banking, and insurance laws, rules, and regulations of this State.

(c) A consumer credit reporting agency that assembles,

evaluates, or maintains a consumer credit report on any consumer located in the State of Illinois at any time between July 1, 2017 and September 1, 2018, shall make the registration required by subsection (a) on or before September 1, 2018. Any other consumer credit reporting agency shall make the registration required by subsection (a) prior to assembling, evaluating, or maintaining a consumer credit report on a consumer located in the State of Illinois.

(d) A consumer credit reporting agency shall renew its registration by January 1, 2019 for the 2019 calendar year, and by January 1 of each successive year for the calendar year thereafter.

(e) The Department may refuse to renew a consumer credit reporting agency's registration if, in the Department's judgment, the applicant or any member, principal, officer or director of the applicant, is not trustworthy and is not competent to act as or in connection with a consumer credit reporting agency, or that any of the foregoing has given cause for revocation or suspension of such registration, or has failed to comply with any minimum standard.

(f) Registrants under this Section shall be subject to examination by the Department as often as the Department may deem it necessary. The Department may promulgate regulations establishing methods and procedures for facilitating and verifying compliance with the requirements of this Act and such other regulations as necessary to enforce the provisions of

this Act.

Section 15. Acting without registration.

(a) No individual, firm, association, corporation or other entity may assemble, evaluate, or maintain a consumer credit report on any consumer located in the State of Illinois without having a valid registration as a consumer credit reporting agency filed as described in Section 10 of this Act.

(b) No financial institution may pay any fee or other compensation to any consumer credit reporting agency that is required to be registered pursuant to Section 10 but fails to possess the required registration.

(c) No regulated person may transmit any information about a consumer located in the State of Illinois to a consumer credit reporting agency that is required to be registered pursuant to Section 10 of this Act but failed to possess the required registration.

Section 20. Revocation and suspension of a registration.

(a) The Department may refuse to renew, revoke, or may suspend the registration of a consumer credit report agency for a period the Department determines if, after notice and hearing, the Department determines that the registrant or any member, principal, officer, director, or controlling person of the registrant, has:

(1) violated any insurance, financial service, or

banking law or violated any regulation, subpoena or order of the Department or any other State or federal agency with authority to regulate consumer credit reporting agencies, or has violated any law in the course of his or her dealings in such capacity;

(2) provided materially incorrect, materially misleading, materially incomplete or materially untrue information in the registration application;

(3) failed to comply with the requirements of this Act, including, but not limited to, Sections 30 through 105 concerning cybersecurity;

(4) used fraudulent, coercive or dishonest practices; demonstrated incompetence; demonstrated untrustworthiness; or demonstrated financial irresponsibility in the conduct of business in this state or elsewhere;

(5) improperly withheld, misappropriated or converted any moneys or properties received in the course of business in this State or elsewhere;

(6) has been convicted of a felony;

(7) admitted or has been found to have committed any unfair trade practice or fraud;

(8) had a consumer credit reporting agency registration or its equivalent, denied, suspended, or revoked in any other state, province, district or territory; or

(9) failed to pay state income tax or comply with any

administrative or court order directing payment of state income tax.

(b) Before revoking or suspending the registration of any consumer credit reporting agency pursuant to the provisions of this Act, the Department shall give notice to the registrant and shall hold, or cause to be held, a hearing not less than 10 days after the giving of such notice.

(c) If a registration pursuant to the provisions of this Act is revoked or suspended by the Department, then the Department shall forthwith give notice to the registrant.

(d) The revocation or suspension of any registration pursuant to the provisions of this Act shall terminate forthwith such registration.

Section 25. Prohibited practices. No consumer credit reporting agency that assembles, evaluates, or maintains a consumer credit report on any consumer located in the State of Illinois shall:

(1) Directly or indirectly employ any scheme, device or artifice to defraud or mislead a consumer.

(2) Engage in any unfair, deceptive, or predatory act or practice toward any consumer, or misrepresent or omit any material information in connection with the assembly, evaluation, or maintenance of a credit report for a consumer located in the State of Illinois.

(3) Engage in any unfair, deceptive, or abusive act or

practice in violation of Section 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

(4) Include inaccurate information in any consumer report relating to a consumer located in the State of Illinois.

(5) Refuse to communicate with an authorized representative of a consumer located in the State of Illinois who provides a written authorization signed by the consumer, provided that the consumer credit reporting agency may adopt procedures reasonably related to verify that the representative is in fact authorized to act on behalf of the consumer.

(6) Make any false statement or make any omission of a material fact in connection with any information or reports filed with a governmental agency or in connection with any investigation conducted by another governmental agency.

Section 30. Cybersecurity program.

(a) By January 1, 2019, a consumer credit reporting agency that assembles, evaluates, or maintains a consumer credit report on Illinois consumers must have in place a written cybersecurity program designed to protect the confidentiality, integrity and availability of the consumer credit reporting agency's information systems.

(b) The cybersecurity program shall be based on the consumer credit reporting agency'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 consumer credit reporting agency's information systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the consumer credit reporting agency'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 consumer credit reporting agency may meet the requirements of this Act by adopting 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 consumer credit reporting agency.

(d) All documentation and information relevant to the consumer credit reporting agency's cybersecurity program shall

be made available to the Department upon request.

Section 35. Cybersecurity policy. Each consumer credit reporting agency shall implement and maintain a written policy or policies, approved by a senior officer, the consumer credit reporting agency's board of directors, an appropriate committee thereof, or equivalent governing body, setting forth the consumer credit reporting agency'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 consumer credit reporting agency's risk assessment and address the following areas to the extent applicable to the consumer credit reporting agency's operations:

(1) information security;

(2) data governance and classification;

(3) asset inventory and device management;

(4) access controls and identity management;

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

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and network monitoring;

(9) systems and application development and quality assurance;

(10) physical security and environmental controls;

(11) consumer data privacy;

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

(13) risk assessment; and

(14) incident response.

Section 40. Chief information officer.

(a) A consumer credit reporting agency shall designate a qualified individual responsible for overseeing and implementing the consumer credit reporting agency's cybersecurity program and enforcing its cybersecurity policy. The chief information security officer may be employed by the consumer credit reporting agency, 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 consumer credit reporting agency shall:

(1) retain responsibility for compliance with this Act;

(2) designate a senior member of the consumer credit reporting agency'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 consumer credit reporting agency in accordance with the requirements of this Act.

(b) The chief information security officer of each consumer

credit reporting agency shall report in writing at least annually to the consumer credit reporting agency's 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 of the consumer credit reporting agency responsible for the consumer credit reporting agency's cybersecurity program. The chief information security officer shall report on the consumer credit reporting agency'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 consumer credit reporting agency's information systems;

(2) the consumer credit reporting agency's cybersecurity policies and procedures;

(3) material cybersecurity risks to the consumer credit reporting agency;

(4) overall effectiveness of the consumer credit reporting agency's cybersecurity program; and

(5) material cybersecurity events involving the consumer credit reporting agency during the time period addressed by the report.

Section 45. Penetration testing and vulnerability assessments. The cybersecurity program for a consumer credit

reporting agency shall include monitoring and testing, developed in accordance with the consumer credit reporting agency's risk assessment, designed to assess the effectiveness of the consumer credit reporting agency'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, consumer credit agencies shall conduct:

(1) annual penetration testing of the consumer credit reporting agency's information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(2) vulnerability assessments every 2 years, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the consumer credit reporting agency's information systems based on the risk assessment.

Section 50. Audit trail.

(a) Each consumer credit reporting agency 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 consumer credit reporting agency; 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 consumer credit reporting agency.

(b) Each consumer credit reporting agency 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 55. Access privileges. As part of its cybersecurity program, based on the consumer credit reporting agency's risk assessment, a consumer credit reporting agency shall limit user access privileges to information systems that provide access to nonpublic information and shall periodically review such access privileges.

Section 60. Application security.

(a) A consumer credit reporting agency'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 consumer credit reporting agency, and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the consumer credit

reporting agency within the context of the consumer credit reporting agency'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 consumer credit reporting agency.

Section 65. Risk assessment.

(a) A consumer credit reporting agency shall conduct a periodic risk assessment of the consumer credit reporting agency's information systems sufficient to inform the designer of the cybersecurity program as required by this Act. Such risk assessment shall be updated as reasonably necessary to address changes to the consumer credit reporting agency's information systems, nonpublic information or business operations. The consumer credit reporting agency's risk assessment shall allow revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the consumer credit reporting agency'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 consumer credit reporting agency;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the consumer credit reporting agency'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 70. Cybersecurity personnel and intelligence.

(a) In addition to the requirements set forth in Section 40, a consumer credit reporting agency shall:

(1) utilize qualified cybersecurity personnel of the consumer credit reporting agency, an affiliate, or a third-party service provider sufficient to manage the consumer credit reporting agency's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in paragraphs (1) through (6) of subsection (b) of Section 30;

(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 consumer credit reporting agency 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 75.

Section 75. Third-party service provider security policy.

(a) Each consumer credit reporting agency 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 consumer credit reporting agency 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 consumer credit reporting agency.

(3) Due diligence processes used to evaluate the adequacy of cybersecurity practices of such third-party service providers.

(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 or contractual protections relating to third-party service providers to the extent applicable 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 80 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 95 of this Act to protect nonpublic information in transit and at rest;

(3) notice to be provided to the consumer credit reporting agency in the event of a cybersecurity event directly impacting the consumer credit reporting agency's information systems or the consumer credit reporting agency'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 consumer credit reporting agency's information systems or nonpublic information.

Section 80. Multi-factor authentication.

(a) Based on its risk assessment, each consumer credit reporting agency 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 consumer credit reporting agency's internal networks from an external network, unless the consumer credit reporting agency's chief information security officer has approved in writing the use of reasonably equivalent or more secure access controls.

Section 85. Limitations on data retention. As part of its cybersecurity program, a consumer credit reporting agency shall include policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes of the consumer credit reporting agency, except where such information 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.

Section 90. Training and monitoring. As part of its cybersecurity program, each consumer credit reporting agency shall:

(1) 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

(2) provide regular cybersecurity awareness training to all personnel that is updated to reflect risks identified by the consumer credit reporting agency in its risk assessment.

Section 95. Encryption of nonpublic information.

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

(1) To the extent a consumer credit reporting agency determines that encryption of nonpublic information in transit over external networks is infeasible, the consumer credit reporting agency may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the consumer credit reporting agency's chief information security officer.

(2) To the extent a consumer credit reporting agency determines that encryption of nonpublic information at

rest is infeasible, the consumer credit reporting agency may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the consumer credit reporting agency's chief information security officer.

(b) To the extent that a consumer credit reporting agency 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 100. Incident response plan.

(a) As part of its cybersecurity program, a consumer credit reporting agency 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 consumer credit reporting agency's information systems or the continuing functionality of any aspect of the consumer credit reporting agency'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 105. Notice to the Department.

(a) A consumer credit reporting agency shall notify the Department 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 consumer credit reporting agency of which notice is required to be provided to a 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 operation of the consumer credit reporting agency.

(b) A consumer credit reporting agency shall submit to the Department a written statement annually covering the prior

calendar year. This statement shall be submitted by February 15th in such manner as determined acceptable by the Department, certifying that the consumer credit reporting agency is in compliance with the requirements set forth in this Act. Each consumer credit reporting agency shall maintain all records, schedules, and data supporting this certificate for a period of 5 years for examination purposes conducted by the Department. To the extent a consumer credit reporting agency has identified areas, systems or processes that require material improvement, updating or redesign, the consumer credit reporting agency 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 Department.

Section 110. Enforcement. This Act shall be enforced by the Department pursuant to, and is not intended to limit, the Department's authority under any applicable laws.

Section 115. Severability. If any provision of this Act or the application thereof to any person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Act or the application thereof to other persons or circumstances.

Section 999. Effective date. This Act takes effect upon

becoming law.