(132nd General Assembly)
(Substitute Senate Bill Number 220)

AN ACT

To amend sections 1306.01 and 3772.01 and to enact sections 1354.01, 1354.02, 1354.03, 1354.04, and 1354.05 of the Revised Code to provide a legal safe harbor to covered entities that implement a specified cybersecurity program, to allow transactions recorded by blockchain technology under the Uniform Electronic Transactions Act, and to alter the definition of "key employee" under the Casino Gaming Law.

Be it enacted by the General Assembly of the State of Ohio:

SECTION 1. That sections 1306.01 and 3772.01 be amended and sections 1354.01, 1354.02, 1354.03, 1354.04, and 1354.05 of the Revised Code be enacted to read as follows:

Sec. 1306.01. As used in sections 1306.01 to 1306.23 of the Revised Code:

(A) "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

(B) "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

(C) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

(D) "Contract" means the total legal obligation resulting from the parties' agreement as affected by sections 1306.01 to 1306.23 of the Revised Code and other applicable law.

(E) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(F) "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

(G) "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means. A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record.

(H) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature.

(I) "Governmental agency" means any executive, legislative, or judicial agency, department,

board, commission, authority, institution, or instrumentality of the federal government, of a state, or of a county, municipality, or other political subdivision of a state.

(J) "Information" means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(K) "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

(L) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(M) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(N) "Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. "Security procedure" includes a procedure that requires the use of algorithms or other codes, identifying word or numbers, encryption, or callback or other acknowledgment procedures.

(O) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. "State" includes an Indian tribe or band, or Alaskan ~~native~~ Native village, that is recognized by federal law or formally acknowledged by a state.

(P) "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Sec. 1354.01. As used in this chapter:

(A) "Business" means any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing.

(B) "Covered entity" means a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state.

(C) "Data breach" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to person or property. "Data breach" does not include either of the following:

(1) Good faith acquisition of personal information or restricted information by the covered entity's employee or agent for the purposes of the covered entity's, provided that the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure;

(2) Acquisition of personal information or restricted information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency.

(D) "Personal information" has the same meaning as in section 1349.19 of the Revised Code.

(E) "Restricted information" means any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property.

As used in this division, "encrypted," "individual," and "redacted" have the same meanings as in section 1349.19 of the Revised Code.

Sec. 1354.02. (A) A covered entity seeking an affirmative defense under sections 1354.01 to 1354.05 of the Revised Code shall do one of the following:

(1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework, as described in section 1354.03 of the Revised Code; or

(2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry recognized cybersecurity framework, as described in section 1354.03 of the Revised Code.

(B) A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in division (A)(1) or (2) of this section, as applicable:

(1) Protect the security and confidentiality of the information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information;

(3) Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

(C) The scale and scope of a covered entity's cybersecurity program under division (A)(1) or (2) of this section, as applicable, is appropriate if it is based on all of the following factors:

(1) The size and complexity of the covered entity;

(2) The nature and scope of the activities of the covered entity;

(3) The sensitivity of the information to be protected;

(4) The cost and availability of tools to improve information security and reduce vulnerabilities;

(5) The resources available to the covered entity.

(D)(1) A covered entity that satisfies divisions (A)(1), (B), and (C) of this section is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information.

(2) A covered entity that satisfies divisions (A)(2), (B), and (C) of this section is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information

security controls resulted in a data breach concerning personal information or restricted information.

Sec. 1354.03. A covered entity's cybersecurity program, as described in section 1354.02 of the Revised Code, reasonably conforms to an industry recognized cybersecurity framework for purposes of that section if division (A), (B), or (C) of this section is satisfied.

(A)(1) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to divisions (A)(2) and (D) of this section:

(a) The "framework for improving critical infrastructure cybersecurity" developed by the "national institute of standards and technology" (NIST);

(b) "NIST special publication 800-171";

(c) "NIST special publications 800-53 and 800-53a";

(d) The "federal risk and authorization management program (FedRAMP) security assessment framework";

(e) The "center for internet security critical security controls for effective cyber defense";

(f) The "international organization for standardization/international electrotechnical commission 27000 family - information security management systems."

(2) When a final revision to a framework listed in division (A)(1) of this section is published, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the revised framework not later than one year after the publication date stated in the revision.

(B)(1) The covered entity is regulated by the state, by the federal government, or both, or is otherwise subject to the requirements of any of the laws or regulations listed below, and the cybersecurity program reasonably conforms to the entirety of the current version of any of the following, subject to division (B)(2) of this section:

(a) The security requirements of the "Health Insurance Portability and Accountability Act of 1996," as set forth in 45 CFR Part 164 Subpart C;

(b) Title V of the "Gramm-Leach-Bliley Act of 1999," Public Law 106-102, as amended;

(c) The "Federal Information Security Modernization Act of 2014," Public Law 113-283;

(d) The "Health Information Technology for Economic and Clinical Health Act," as set forth in 45 CFR part 162.

(2) When a framework listed in division (B)(1) of this section is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the amended framework not later than one year after the effective date of the amended framework.

(C)(1) The cybersecurity program reasonably complies with both the current version of the "payment card industry (PCI) data security standard" and conforms to the current version of another applicable industry recognized cybersecurity framework listed in division (A) of this section, subject to divisions (C)(2) and (D) of this section.

(2) When a final revision to the "PCI data security standard" is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply with the revised standard not later than one year after the publication date stated in the revision.

(D) If a covered entity's cybersecurity program reasonably conforms to a combination of industry recognized cybersecurity frameworks, or complies with a standard, as in the case of the payment card industry (PCI) data security standard, as described in division (A) or (C) of this

section, and two or more of those frameworks are revised, the covered entity whose cybersecurity program reasonably conforms to or complies with, as applicable, those frameworks shall reasonably conform to or comply with, as applicable, all of the revised frameworks not later than one year after the latest publication date stated in the revisions.

Sec. 1354.04. Sections 1354.01 to 1354.05 of the Revised Code shall not be construed to provide a private right of action, including a class action, with respect to any act or practice regulated under those sections.

Sec. 1354.05. If any provision of sections 1354.01 to 1354.05 of the Revised Code or the application thereof to a covered entity is for any reason held to be invalid, the remainder of the provisions under those sections and the application of such provisions to other covered entities shall not be thereby affected.

Sec. 3772.01. As used in this chapter:

(A) "Applicant" means any person who applies to the commission for a license under this chapter.

(B) "Casino control commission fund" means the casino control commission fund described in Section 6(C)(3)(d) of Article XV, Ohio Constitution, the money in which shall be used to fund the commission and its related affairs.

(C) "Casino facility" means a casino facility as defined in Section 6(C)(9) of Article XV, Ohio Constitution.

(D) "Casino game" means any slot machine or table game as defined in this chapter.

(E) "Casino gaming" means any type of slot machine or table game wagering, using money, casino credit, or any representative of value, authorized in any of the states of Indiana, Michigan, Pennsylvania, and West Virginia as of January 1, 2009, and includes slot machine and table game wagering subsequently authorized by, but shall not be limited by, subsequent restrictions placed on such wagering in such states. "Casino gaming" does not include bingo, as authorized in Section 6 of Article XV, Ohio Constitution and conducted as of January 1, 2009, or horse racing where the pari-mutuel system of wagering is conducted, as authorized under the laws of this state as of January 1, 2009.

(F) "Casino gaming employee" means any employee of a casino operator or management company, but not a key employee, and as further defined in section 3772.131 of the Revised Code.

(G) "Casino operator" means any person, trust, corporation, partnership, limited partnership, association, limited liability company, or other business enterprise that directly or indirectly holds an ownership or leasehold interest in a casino facility. "Casino operator" does not include an agency of the state, any political subdivision of the state, any person, trust, corporation, partnership, limited partnership, association, limited liability company, or other business enterprise that may have an interest in a casino facility, but who is legally or contractually restricted from conducting casino gaming.

(H) "Central system" means a computer system that provides the following functions related to casino gaming equipment used in connection with casino gaming authorized under this chapter: security, auditing, data and information retrieval, and other purposes deemed necessary and authorized by the commission.

(I) "Cheat" means to alter the result of a casino game, the element of chance, the operation of

a machine used in a casino game, or the method of selection of criteria that determines (a) the result of the casino game, (b) the amount or frequency of payment in a casino game, (c) the value of a wagering instrument, or (d) the value of a wagering credit. "Cheat" does not include an individual who, without the assistance of another individual or without the use of a physical aid or device of any kind, uses the individual's own ability to keep track of the value of cards played and uses predictions formed as a result of the tracking information in the individual's playing and betting strategy.

(J) "Commission" means the Ohio casino control commission.

(K) "Gaming agent" means a peace officer employed by the commission that is vested with duties to enforce this chapter and conduct other investigations into the conduct of the casino gaming and the maintenance of the equipment that the commission considers necessary and proper and is in compliance with section 109.77 of the Revised Code.

(L) "Gaming-related vendor" means any individual, partnership, corporation, association, trust, or any other group of individuals, however organized, who supplies gaming-related equipment, goods, or services to a casino operator or management company, that are directly related to or affect casino gaming authorized under this chapter, including, but not limited to, the manufacture, sale, distribution, or repair of slot machines and table game equipment.

(M) "Holding company" means any corporation, firm, partnership, limited partnership, limited liability company, trust, or other form of business organization not a natural person which directly or indirectly does any of the following:

(1) Has the power or right to control a casino operator, management company, or gaming-related vendor license applicant or licensee;

(2) Holds an ownership interest of five per cent or more, as determined by the commission, in a casino operator, management company, or gaming-related vendor license applicant or licensee;

(3) Holds voting rights with the power to vote five per cent or more of the outstanding voting rights of a casino operator, management company, or gaming-related vendor applicant or licensee.

(N) "Initial investment" includes costs related to demolition, engineering, architecture, design, site preparation, construction, infrastructure improvements, land acquisition, fixtures and equipment, insurance related to construction, and leasehold improvements.

(O) "Institutional investor" means any of the following entities owning five per cent or more, but less than fifteen per cent, of an ownership interest in a casino facility, casino operator, management company, or holding company: a corporation, bank, insurance company, pension fund or pension fund trust, retirement fund, including funds administered by a public agency, employees' profit-sharing fund or employees' profit-sharing trust, any association engaged, as a substantial part of its business or operations, in purchasing or holding securities, including a hedge fund, mutual fund, or private equity fund, or any trust in respect of which a bank is trustee or cotrustee, investment company registered under the "Investment Company Act of 1940," 15 U.S.C. 80a-1 et seq., collective investment trust organized by banks under Part Nine of the Rules of the Comptroller of the Currency, closed-end investment trust, chartered or licensed life insurance company or property and casualty insurance company, investment advisor registered under the "Investment Advisors Act of 1940," 15 U.S.C. 80 b-1 et seq., and such other persons as the commission may reasonably determine to qualify as an institutional investor for reasons consistent with this chapter, and that does not exercise control over the affairs of a licensee and its ownership interest in a licensee is for investment purposes only,

as set forth in division (E) of section 3772.10 of the Revised Code.

(P) "Key employee" means any executive, employee, ~~or~~ agent, or other individual who has the power to exercise significant influence over decisions concerning any part of the operation of a person that has applied for or holds a casino operator ~~or~~, management company ~~licensee having the power to exercise significant influence over decisions concerning any part of the operation of such licensee~~, or gaming-related vendor license or the operation of a holding company of a person that has applied for or holds a casino operator, management company, or gaming-related vendor license, including:

(1) An officer, director, trustee, ~~or~~ partner ~~of a person that has applied for or holds a casino operator, management company, or gaming-related vendor license or of a holding company that has control of a person that has applied for or holds a casino operator, management company, or gaming-related vendor license~~, or an equivalent fiduciary;

(2) ~~A person that~~ An individual who holds a direct or indirect ownership interest of ~~more than one~~ five per cent ~~in a person that has applied for or holds a casino operator, management company, or gaming-related vendor license or holding company that has control of a person that has applied for or holds a casino operator, management company, or gaming-related vendor license~~ or more;

(3) ~~A managerial employee of a person that has applied for or holds a casino operator or gaming-related vendor license in Ohio, or a managerial employee of a holding company that has control of a person that has applied for or holds a casino operator or gaming-related vendor license in Ohio,~~ An individual who performs the function of a principal executive officer, principal operating officer, principal accounting officer, or an equivalent officer ~~or~~ ;

(4) Any other ~~person~~ individual the commission determines to have the power to exercise significant influence over decisions concerning any part of the operation ~~of such licensee~~.

~~The commission shall determine whether an individual whose duties or status varies from those described in this division also is considered a key employee.~~

(Q) "Licensed casino operator" means a casino operator that has been issued a license by the commission and that has been certified annually by the commission to have paid all applicable fees, taxes, and debts to the state.

(R) "Majority ownership interest" in a license or in a casino facility, as the case may be, means ownership of more than fifty per cent of such license or casino facility, as the case may be. For purposes of the foregoing, whether a majority ownership interest is held in a license or in a casino facility, as the case may be, shall be determined under the rules for constructive ownership of stock provided in Treas. Reg. 1.409A-3(i)(5)(iii) as in effect on January 1, 2009.

(S) "Management company" means an organization retained by a casino operator to manage a casino facility and provide services such as accounting, general administration, maintenance, recruitment, and other operational services.

(T) "Ohio law enforcement training fund" means the state law enforcement training fund described in Section 6(C)(3)(f) of Article XV, Ohio Constitution, the money in which shall be used to enhance public safety by providing additional training opportunities to the law enforcement community.

(U) "Person" includes, but is not limited to, an individual or a combination of individuals; a sole proprietorship, a firm, a company, a joint venture, a partnership of any type, a joint-stock

company, a corporation of any type, a corporate subsidiary of any type, a limited liability company, a business trust, or any other business entity or organization; an assignee; a receiver; a trustee in bankruptcy; an unincorporated association, club, society, or other unincorporated entity or organization; entities that are disregarded for federal income tax purposes; and any other nongovernmental, artificial, legal entity that is capable of engaging in business.

(V) "Problem casino gambling and addictions fund" means the state problem gambling and addictions fund described in Section 6(C)(3)(g) of Article XV, Ohio Constitution, the money in which shall be used for treatment of problem gambling and substance abuse, and for related research.

(W) "Promotional gaming credit" means a slot machine or table game credit, discount, or other similar item issued to a patron to enable the placement of, or increase in, a wager at a slot machine or table game.

(X) "Slot machine" means any mechanical, electrical, or other device or machine which, upon insertion of a coin, token, ticket, or similar object, or upon payment of any consideration, is available to play or operate, the play or operation of which, whether by reason of the skill of the operator or application of the element of chance, or both, makes individual prize determinations for individual participants in cash, premiums, merchandise, tokens, or any thing of value, whether the payoff is made automatically from the machine or in any other manner, but does not include any device that is a skill-based amusement machine, as defined in section 2915.01 of the Revised Code.

(Y) "Table game" means any game played with cards, dice, or any mechanical, electromechanical, or electronic device or machine for money, casino credit, or any representative of value. "Table game" does not include slot machines.

(Z) "Upfront license" means the first plenary license issued to a casino operator.

(AA) "Voluntary exclusion program" means a program provided by the commission that allows persons to voluntarily exclude themselves from the gaming areas of facilities under the jurisdiction of the commission by placing their name on a voluntary exclusion list and following the procedures set forth by the commission.

SECTION 2. That existing sections 1306.01 and 3772.01 of the Revised Code are hereby repealed.

SECTION 3. (A) The purpose of this act is to establish a legal safe harbor to be pled as an affirmative defense to a cause of action sounding in tort that alleges or relates to the failure to implement reasonable information security controls, resulting in a data breach. The safe harbor shall apply to all covered entities that implement a cybersecurity program that meets the requirements of the act.

(B) This act is intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action. The act does not, and is not intended to, create a minimum cybersecurity standard that must be achieved, nor shall it be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the act.

_____

Speaker _____ of the House of Representatives.

_____

President _____ of the Senate.

Passed _____, 20____

Approved _____, 20____

_____

Governor.

The section numbering of law of a general and permanent nature is complete and in conformity with the Revised Code.

_____

Director, Legislative Service Commission.

Filed in the office of the Secretary of State at Columbus, Ohio, on the ____ day of _____, A. D. 20____.

_____

Secretary of State.

File No. _____ Effective Date _____