As Introduced

126th General Assembly
Regular Session **H. B. No. 104**
2005-2006

Representatives Martin, McGregor, Trakas, Wagoner, C. Evans, Perry, Seitz

A B I L L

To amend section 1347.01 and to enact sections 1347.12 and 1349.19 of the Revised Code to require a state agency, person, or business to contact individuals if unencrypted personal information about those individuals that is maintained on the computers of the agency, person, or business is obtained by unauthorized persons.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF OHIO:

Section 1. That section 1347.01 be amended and sections 1347.12 and 1349.19 of the Revised Code be enacted to read as follows:

Sec. 1347.01. As used in this chapter, except as otherwise provided:

(A) "State agency" means the office of any elected state officer and any agency, board, commission, department, division, or educational institution of the state.

(B) "Local agency" means any municipal corporation, school district, special purpose district, or township of the state or any elected officer or board, bureau, commission, department, division, institution, or instrumentality of a county.

(C) "Special purpose district" means any geographic or political jurisdiction that is created by statute to perform a limited and specific function, and includes, but is not limited to, library districts, conservancy districts, metropolitan housing authorities, park districts, port authorities, regional airport authorities, regional transit authorities, regional water and sewer districts, sanitary districts, soil and water conservation districts, and regional planning agencies.

(D) "Maintains" means state or local agency ownership of, control over, responsibility for, or accountability for systems and includes, but is not limited to, state or local agency depositing of information with a data processing center for storage, processing, or dissemination. An agency "maintains" all systems of records that are required by law to be kept by the agency.

(E) "Personal information" means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.

(F) "System" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved by the name of the person or by some identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment. "System" does not include collected archival records in the custody of or administered under the authority of the Ohio historical society, published directories, reference materials or newsletters, or routine information that is maintained for the purpose of internal

office administration, the use of which would not adversely affect a person.

(G) "Interconnection of systems" means a linking of systems that belong to more than one agency, or to an agency and other organizations, which linking of systems results in a system that permits each agency or organization involved in the linking to have unrestricted access to the systems of the other agencies and organizations.

(H) "Combination of systems" means a unification of systems that belong to more than one agency, or to an agency and another organization, into a single system in which the records that belong to each agency or organization may or may not be obtainable by the others.

Sec. 1347.12. (A) As used in this section:

(1) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state agency. Good faith acquisition of personal information by an employee or agent of the state agency for the purposes of the state agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(2) "Individual" means a natural person.

(3) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or state identification card number;

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(4) "State agency" has the same meaning as in section 1.60 of the Revised Code.

(B)(1) Any state agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of this state whose unencrypted personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

(2) The state agency shall make the disclosure described in division (B)(1) of this section in the most expedient time possible and without unreasonable delay, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(C) Any state agency that maintains computerized data that includes personal information that the state agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

(D) The state agency may delay the disclosure or notification required by division (B) or (C) of this section if a law enforcement agency determines that the disclosure or notification

will impede a criminal investigation, in which case, the state agency shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation.

(E) For purposes of this section, a state agency may disclose or make a notification by the following methods:

(1) Written notice;

(2) Electronic notice, if the disclosure or notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as amended.

(3) Notice consisting of all of the following:

(a) Electronic mail notice when the state agency has electronic mail addresses for the subject persons requiring disclosure or notification;

(b) Conspicuous posting of the disclosure or notice on the state agency's website, if the agency maintains one;

(c) Notification to major statewide media.

(F) Notwithstanding division (E) of this section, a state agency that maintains its own disclosure or notification procedures as part of an information security policy for the treatment of personal information, which procedures also are consistent with the timing requirements of this section, is in compliance with the disclosure or notification requirements of this section, if it notifies subject persons requiring disclosure or notification in accordance with its policies in the event of a breach of the security of the system.

Sec. 1349.19. (A) As used in this section:

(1) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security,

confidentiality, or integrity of personal information maintained by a person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(2) "Business" means both of the following:

(a) A sole proprietorship, partnership, corporation, 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 a financial institution;

(b) An entity that destroys records.

(3) "Individual" means a natural person.

(4) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or state identification card number;

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(5) "Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted. "Records" does not include publicly available directories containing information an individual voluntarily has consented to have publicly disseminated or listed, such as name, address, or telephone number.

(B)(1) Any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of this state whose unencrypted personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

(2) The person or business shall make the disclosure described in division (B)(1) of this section in the most expedient time possible and without unreasonable delay, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(C) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

(D) The person or business may delay the disclosure or notification required by division (B) or (C) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation, in which case,

the person or business shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation.

(E) For purposes of this section, a person or business may disclose or make a notification by the following methods:

(1) Written notice;

(2) Electronic notice, if the disclosure or notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as amended.

(3) Notice consisting of all of the following:

(a) Electronic mail notice when the person or business has electronic mail addresses for the subject persons requiring disclosure or notification;

(b) Conspicuous posting of the disclosure or notice on the person's or business' website, if the person or business maintains one;

(c) Notification to major statewide media.

(F) Notwithstanding division (E) of this section, a person or business that maintains its own disclosure or notification procedures as part of an information security policy for the treatment of personal information, which procedures also are consistent with the timing requirements of this section, is in compliance with the disclosure or notification requirements of this section, if the person or business notifies subject persons requiring disclosure or notification in accordance with its policies in the event of a breach of the security of the system.

(G) Any waiver of this section is contrary to public policy and is void and unenforceable.

(H) Any individual injured by a violation of this section has a cause of action for recovery of damages.

Section 2. That existing section 1347.01 of the Revised Code is hereby repealed.