Aida S. Montano *Legislative Service Commission*

H.B. 104

126th General Assembly
(As Introduced)

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

BILL SUMMARY

- Requires any state agency that owns or licenses computerized data that includes personal information to disclose, in the most expedient time possible and without unreasonable delay, any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any Ohio resident whose unencrypted personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

- Requires any state agency that maintains computerized data that includes personal information that the state agency does not own to 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.

- Requires any person or business that conducts business in Ohio and that owns or licenses computerized data that includes personal information to disclose, in the most expedient time possible and without unreasonable delay, any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any Ohio resident whose unencrypted personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

- Requires any person or business that maintains computerized data that includes personal information that the person or business does not own to 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.

- Permits a state agency or any person or business, whichever is applicable, to delay the required disclosure or notification if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation.

- Specifies the methods by which a state agency or any person or business, as the case may be, may disclose or make a notification as required by the bill, and provides that notwithstanding those methods, a state agency or any person or business, whichever is applicable, that maintains its own disclosure or notification procedures as part of a personal information security policy, which procedures are consistent with the bill's timing requirements, is in compliance with the bill's disclosure or notification requirements, if it notifies subject persons in accordance with its policies in case of a breach of the security of the system.

- Provides that any waiver of the bill's provisions pertaining to the required disclosure and notification by *any person or business* is contrary to public policy and is void and unenforceable.

- Grants a cause of action for damages to any individual injured by a violation of the provisions pertaining to the required disclosure and notification by *any person or business*.

TABLE OF CONTENTS

CONTENT AND OPERATION

Disclosure or notification by state agency of breach of security of personal information system

The bill generally provides for a state agency's disclosure to Ohio residents of any breach of security of the agency's computerized data that includes personal information or notification of any such breach of security to the owner or licensee of personal information maintained by the state agency.

Requirement for disclosure or notification

The bill requires any "state agency" that *owns or licenses* computerized data that includes "personal information" to 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 Ohio whose unencrypted personal information was, or reasonably is believed to have been, acquired by an unauthorized person. (See "***Definitions for purposes of disclosure or notification by state agency***," below, for definitions of the terms in quotation marks.) The state agency must make that disclosure in the most expedient time possible and without unreasonable delay, subject to the legitimate needs of law enforcement activities described below, and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. (R.C. 1347.12(B).)

The bill also requires any state agency that maintains computerized data that includes personal information that the state agency *does not own* to 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 (R.C. 1347.12(C)).

The bill permits the state agency to delay the required disclosure or notification described in the two preceding paragraphs if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation, in which case, the state agency must make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation (R.C. 1347.12(D)).

Methods of disclosure or notification

The bill provides that a state agency may disclose or make a notification as described above by the following methods (R.C. 1347.12(E)):

(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 (Electronic Signatures in Global and National Commerce Act) (see **COMMENT**);

(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, and (c) notification to major statewide media.

The bill provides that notwithstanding the above methods for making a disclosure or notification, 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 the bill, is in compliance with the bill's disclosure or notification requirements, 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 (R.C. 1347.12(F)).

Definitions for purposes of disclosure or notification by state agency

The bill defines the following terms for purposes of its provisions requiring a state agency to make the disclosure or notification described above (R.C. 1347.12(A)):

"State agency" means every organized body, office, or agency established by the laws of Ohio for the exercise of any function of state government (R.C. 1.60).

"Personal information" means an individual's (defined as a natural person) 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: (1) social security number, (2) driver's license number or state identification card number, (3) 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.

"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.

Disclosure or notification by any person or business of breach of security of personal information system

The bill generally provides for the disclosure by any person or business conducting business in Ohio to residents of Ohio of any breach of security of computerized data that includes personal information.

Requirement for disclosure or notification

The bill requires any person or "business" that conducts business in Ohio and that *owns or licenses* computerized data that includes "personal information" to 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 Ohio whose unencrypted personal information was, or reasonably is believed to have been, acquired by an unauthorized person. (See "***Definitions for purposes of disclosure or notification by any person or business***," below, for definitions of the terms in quotation marks.) The person or business must make the required disclosure in the most expedient time possible and without unreasonable delay, subject to the legitimate needs of law enforcement activities described below and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. (R.C. 1349.19(B).)

The bill also requires any person or business that maintains computerized data that includes personal information that the person or business *does not own* to 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 (R.C. 1349.19(C)).

The bill permits any person or business to delay the required disclosure or notification as described in the two preceding paragraphs if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation, in which case, the person or business must make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation (R.C. 1349.19(D)).

Methods of disclosure or notification

The bill provides that a person or business may disclose or make a notification as described above by the following methods (R.C. 1349.19(E)):

(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 (Electronic Signatures in Global and National Commerce Act) (see **COMMENT**);

(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, and (c) notification to major statewide media.

The bill provides that notwithstanding the above methods for making a disclosure or notification, 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 the bill, is in compliance with the bill's disclosure or notification requirements, 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 (R.C. 1349.19(F)).

Nonwaivable duties

The bill provides that any waiver of the above provisions requiring disclosure or notification by a person or business is contrary to public policy and is void and unenforceable (R.C. 1349.19(G)).

Cause of action

The bill provides that any individual injured by a violation of any of the above provisions requiring disclosure or notification by a person or business has a cause of action for recovery of damages (R.C. 1349.19(H)).

Definitions for purposes of disclosure or notification by any person or business

The bill defines the following terms for purposes of its provisions requiring any person or business to make the above described disclosure or notification (R.C. 1349.19(A)):

"Business" means both of the following:

(1) 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 Ohio, any other state, the United States, or any other country, or the parent or subsidiary of a financial institution;

(2) An entity that destroys records.

"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.

"Personal information" is defined in the same manner as the definition of "personal information" in "***Definitions for purposes of disclosure or notification by state agency***," above.

"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.

COMMENT

Existing 15 U.S.C. 7001, not in the bill, provides as follows:

> **(a) In general**
>
> Notwithstanding any statute, regulation, or other rule of law (other than this subchapter and subchapter II of this chapter) with respect to any transaction in or affecting interstate or foreign commerce--
>
> **(1)** a signature, contract, or other record relating to such transaction may not be denied legal

effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

(b) Preservation of rights and obligations

This subchapter does not--

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

(c) Consumer disclosures

(1) Consent to electronic records

Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if--

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement--

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer--

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a

subsequent electronic record that was the subject of the consent, the person providing the electronic record--

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(2) Other rights

(A) Preservation of consumer protections

Nothing in this subchapter affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, regulation, or other rule of law.

(B) Verification or acknowledgment

If a law that was enacted prior to this chapter [enacted June 30, 2000] expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

(3) Effect of failure to obtain electronic consent or confirmation of consent

The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) Prospective effect

Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) Prior consent

This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) Oral communications

An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

(d) Retention of contracts and records

(1) Accuracy and accessibility

If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that--

(A) accurately reflects the information set forth in the contract or other record; and

(B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law,

for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) Exception

A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) Originals

If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with paragraph (1).

(4) Checks

If a statute, regulation, or other rule of law requires the retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with paragraph (1).

(e) Accuracy and ability to retain contracts and other records

Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later

reference by all parties or persons who are entitled to retain the contract or other record.

(f) Proximity

Nothing in this subchapter affects the proximity required by any statute, regulation, or other rule of law with respect to any warning, notice, disclosure, or other record required to be posted, displayed, or publicly affixed.

(g) Notarization and acknowledgment

If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

(h) Electronic agents

A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.

(i) Insurance

It is the specific intent of the Congress that this subchapter and subchapter II of this chapter apply to the business of insurance.

(j) Insurance agents and brokers

An insurance agent or broker acting under the direction of a party that enters into a contract by means of an electronic record or electronic signature may not

be held liable for any deficiency in the electronic procedures agreed to by the parties under that contract if--

(1) the agent or broker has not engaged in negligent, reckless, or intentional tortious conduct;

(2) the agent or broker was not involved in the development or establishment of such electronic procedures; and

(3) the agent or broker did not deviate from such procedures.

HISTORY

ACTION	DATE	JOURNAL ENTRY
Introduced	03-01-05	p. 240

H0104-I-126.doc/jc