Sub. H.B. 104

126th General Assembly
(As Passed by the House)

Reps. Martin, McGregor, Trakas, Wagoner, C. Evans, Perry, Seitz, Coley, Core, Harwood, Allen, Beatty, Blessing, Bubp, Buehrer, Carano, Cassell, Collier, DeBose, DeGeeter, Distel, Dolan, Domenick, Faber, Fende, Fessler, Flowers, Gibbs, Gilb, Hughes, Kearns, Latta, Mason, Miller, Oelslager, Otterman, S. Patton, T. Patton, Raussen, Reidelbach, Reinhard, Sayre, Schaffer, Schneider, Seaver, Setzer, Skindell, G. Smith, S. Smith, D. Stewart, J. Stewart, Strahorn, Williams

BILL SUMMARY

- Requires any state agency that maintains computerized data that includes personal information of a specified nature to disclose, in the most expedient time possible but generally not later than 45 days following its discovery or notification of the security breach, any breach of the security of the system to any Ohio resident whose personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

- Requires any state agency that on behalf of another state agency maintains computerized data that includes personal information of a specified nature to notify that other state agency of any breach of the security of the system in an expeditious manner, 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 maintains computerized data that includes personal information of a specified nature to disclose, in the most expedient time possible but generally not later than 45 days following its discovery or notification of the security breach, any breach of the security of the system, to any Ohio resident whose personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

- Requires any person or business that on behalf of another person or business maintains computerized data that includes personal information

of a specified nature to notify that other person or business of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, acquired by an unauthorized person.

- Permits a state agency, 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, person, or business may disclose or make a notification as required by the bill, and provides that, notwithstanding those methods, a state agency, person, or business, whichever is applicable, that maintains its own disclosure or notification procedures as part of a personal information privacy or 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.

- Requires a state agency, person, or business, whichever is applicable, that discovers circumstances requiring disclosure to more than 1,000 Ohio residents involved in a single occurrence of a breach of the security of the system to notify without unreasonable delay all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given to Ohio residents pursuant to the bill.

- Provides that any financial institution, trust company, or credit union or affiliate of any of those entities that is required by federal law to notify its customers of an information security breach with respect to information about those customers and that is subject to its government regulatory agency's examination for compliance with that law is exempt from the bill's requirements with respect to disclosure by *any person or business*.

- Provides that the bill's provisions pertaining to the required disclosure and notification by *any person or business* do not apply to any person or entity regulated by the Health Insurance Portability and Accountability Act (HIPAA).

- 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.

- Authorizes the Attorney General to conduct an investigation and grants the Attorney General subpoena authority if the Attorney General has reason to believe that a state agency, person, or business has failed or is failing to comply with the bill's requirements, and prescribes procedures upon issuance of a subpoena by a court.

- Authorizes the Attorney General to bring a civil action in a court of common pleas if it appears that a state agency, person, or business has failed or is failing to comply with the bill's requirements and requires the court, upon a finding of such failure, to impose a civil penalty of not more than $1,000 per day for each day the state agency, person, or business fails to comply with the bill.

- Provides that any civil penalty assessed as described in the preceding dot point must be deposited into the Consumer Protection Enforcement Fund for the sole purpose of paying expenses incurred by the Consumer Protection Section of the Attorney General's Office.

- States that it deals with a matter of statewide concern and that the General Assembly intends that the bill supersede and preempt all local rules, regulations, resolutions, codes, and ordinances that pertain to matters expressly set forth or regulated under the bill.

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 another state agency on behalf of which computerized data that includes personal information is maintained by the state agency.

Requirement for disclosure or notification

The bill requires any "state agency" that "maintains" computerized data that includes "personal information" to disclose any "breach of the security of the system," following its discovery or notification of the breach of the security of the system, to any resident of Ohio whose 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 disclosure may be made pursuant to any provision of a contract entered into by the state agency with any person or another state agency prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of the bill regarding state agency disclosure. For the purposes of this provision, a resident of Ohio is an individual whose principal mailing address as reflected in the records of the state agency is in Ohio. The state agency must make that disclosure in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system, 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 on behalf of another state agency maintains computerized data that includes personal information to notify that other state agency of any breach of the security of the system in an expeditious manner, 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 any of 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) telephone notice, or (4) notice consisting of all of the following: electronic mail notice when the state agency has electronic mail addresses for the subject persons requiring disclosure or notification; conspicuous posting of the disclosure or notice on the state agency's website, if the agency maintains one; and 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 privacy or security policy for the treatment of personal information, which procedures also are consistent with the timing requirements of the bill's provisions regarding state agency disclosure, 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)).

Disclosure or notification of breach of security of system involving more than 1,000 persons: consumer reporting agencies

The bill provides that, if a state agency discovers circumstances that require disclosure under the bill's provisions regarding state agency disclosure to more than 1,000 Ohio residents involved in a single occurrence of a breach of the security of the system, the state agency must notify, without unreasonable delay, all "consumer reporting agencies that compile and maintain files on consumers on a nationwide basis" (see "***Definitions for purposes of disclosure or notification by***

state agency," below) of the timing, distribution, and content of the disclosure given by the state agency to the Ohio residents (R.C. 1347.12(G)).

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 (by reference to existing R.C. 1.60, not in the bill).

"***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, redacted, or altered by any method or technology: (1) Social Security Number, (2) driver's license number or state identification card number, or (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 or widely distributed media.

"***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 and that causes or reasonably is believed to cause injury or loss to the person or property of a resident of Ohio. 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. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order is not a breach of the security of the system.

"***Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis***" means a consumer reporting agency that, for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity, regularly engages in the practice of assembling or evaluating, and maintaining, each of the following regarding consumers residing nationwide: (1) public record information, and (2) credit account information from persons who furnish that information to the credit reporting agency regularly and in the ordinary course of business.

Existing law defines the following terms, and the definitions apply to the provisions requiring a state agency to make the disclosure or notification described above (R.C. 1347.01(D) and (F), unchanged by the bill--definitions of terms used in R.C. Chapter 1347. (Personal Information Systems Law), which includes the bill's provisions)[1]:

"***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.

"***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.

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 "maintains" computerized data that includes "personal information" to disclose any "breach of the security of the system," following its discovery or notification of the breach of the security of the system, to any resident of Ohio whose 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

[1] *The definitions of "maintains" and "system" in R.C. 1347.01(D) refer to a* state or local agency. *For purposes of the bill, these existing definitions apply only with respect to a* state agency *that maintains a system.*

quotation marks.) The disclosure may be made pursuant to any provision of a contract entered into by the person or business with another person or business prior to the date the breach of the security of the system occurred if that contract does not conflict with or waive any provision of the bill regarding person and business disclosure. For the purposes of this provision, a resident of Ohio is an individual whose principal mailing address as reflected in the records of the person or business is in Ohio. The person or business must make the required disclosure in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system, 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 on behalf of another person or business maintains computerized data that includes personal information to notify that other person or business of any breach of the security of the system in an expeditious manner, 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 any of 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) telephone notice, or (4) notice consisting of all of the following: electronic mail notice when the person or business has electronic mail addresses for the subject persons requiring disclosure or notification; conspicuous posting of the disclosure or notice on the person's or business' website, if the person or business maintains one; and 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 privacy or security policy for the treatment of personal information, which procedures also are consistent with the

timing requirements of the bill's provisions regarding person and business disclosure, 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)(1)).

The bill provides that a financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the bill's requirements regarding person and business disclosure (R.C. 1349.19(F)(2)).

Disclosure or notification of breach of security of system involving more than 1,000 persons: consumer reporting agencies

The bill provides that, if a person or business discovers circumstances that require disclosure under the bill's provisions regarding person and business disclosure to more than 1,000 Ohio residents involved in a single occurrence of a breach of the security of the system, the person or business must notify, without unreasonable delay, all "consumer reporting agencies that compile and maintain files on consumers on a nationwide basis" (see "***Definitions for purposes of disclosure or notification by any person or business***," below) of the timing, distribution, and content of the disclosure given by the person or business to the Ohio residents (R.C. 1349.19(G)).

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(H)).

Application of bill

The bill provides that the above provisions regarding person and business disclosure do not apply to any person or entity regulated by sections 1171 to 1179 of the Social Security Act (Health Insurance Portability and Accountability Act or HIPAA) and any corresponding regulations (R.C. 1349.19(F)(3)).

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***" and "***Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis***" are defined in the same manner as the definition of those terms 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 and that causes or reasonably is believed to cause injury or loss to the person or property of a resident of this state. 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. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order is not a breach of the security of the system.

"***Maintains***" means a person's or business's ownership of, control over, responsibility for, or accountability for systems and includes, but is not limited to, a person's or business's depositing of information with a data processing center for

storage, processing, or dissemination. A person or business "maintains" all systems of records that are required by law to be kept by the person or business.

"***System***" means any collection or group of related records that are kept in an organized manner, that are maintained by a state or business, 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 published directories, reference materials or newsletters, or routine information that is maintained for the purpose of internal office administration of the person or business and the use of which would not adversely affect a person.

Investigation and enforcement by Attorney General

Investigation

The bill authorizes the Attorney General (AG) to conduct an investigation if the AG, based on complaints or the AG's own inquiries, has reason to believe that a state agency, person, or business has failed or is failing to comply with the respective disclosure requirements of the bill, as described above. In any such investigation, the AG may administer oaths, subpoena witnesses, adduce evidence, and subpoena the production of any book, document, record, or other relevant matter. If the AG subpoenas the production of any relevant matter that is located outside Ohio, the AG may designate a representative, including an official of the state in which that matter is located, to inspect the matter on the AG's behalf. The AG may carry out similar requests received from officials of other states. Any person who is subpoenaed to produce relevant matter must make that matter available at a convenient location in Ohio or the state of the representative designated as described above. (R.C. 1349.191(B), (C), and (D), 1347.12(H), and 1349.19(I).)

Court procedure upon subpoena

Any person who is subpoenaed as a witness or to produce relevant matter may file in the Court of Common Pleas of Franklin County, the county in Ohio in which the person resides, or the county in Ohio in which the person's principal place of business is located a petition to extend for good cause shown the date on which the subpoena is to be returned or to modify or quash for good cause shown that subpoena. The person may file the petition at any time prior to the date specified for the return of the subpoena or within 20 days after the service of the subpoena, whichever is earlier. Any person who is subpoenaed as a witness or to produce relevant matter under the provisions described in the preceding paragraph must comply with the terms of the subpoena unless the court orders otherwise

prior to the date specified for the return of the subpoena or, if applicable, that date as extended. If a person fails without lawful excuse to obey a subpoena, the AG may apply to the court of common pleas for an order that does one or more of the following: (1) compels the requested discovery, (2) adjudges the person in contempt of court, (3) grants injunctive relief to restrain the person from failing to comply with the applicable disclosure requirements, (4) grants injunctive relief to preserve or restore the status quo, or (5) grants other relief that may be required until the person obeys the subpoena. The court must impose a civil penalty on any person who violates a court order issued as described above. The civil penalty is to be not more than $1,000 per day for each day the person is violating the court order. (R.C. 1349.191(E), (F), and (G) and 1349.192(A).)

Civil action

The bill authorizes the AG to bring a civil action in a court of common pleas for appropriate relief, including a temporary restraining order, preliminary or permanent injunction, and civil penalties, if it appears that a state agency, person, or business has failed or is failing to comply with the respective disclosure requirements of the bill. Upon its findings of such a failure to comply, the court must impose a civil penalty of not more than $1,000 per day for each day the state agency or the person or business fails to comply with the applicable disclosure requirements. Any civil penalty that is assessed under this provision must be deposited into the Consumer Protection Enforcement Fund to be used for the sole purpose of paying expenses incurred by the Consumer Protection Section of the AG's Office. (R.C. 1349.192(A), 1347.12(H), 1349.19(I), and 1345.51.)

Any state agency or any person or business that is found by the court to have failed to comply with the applicable disclosure requirements in the bill is liable to the AG for the costs in conducting an investigation and bringing an action under the bill (R.C. 1349.192(B)).

The above rights and remedies are in addition to any other rights and remedies that are provided by law (R.C. 1349.192(C)).

Statewide concern--preemption

The bill states that it deals with a subject matter of statewide concern. It also states that it is the intent of the General Assembly that the bill supersede and preempt all rules, regulations, resolutions, codes, and ordinances of all counties, municipal corporations, townships, and agencies of counties, municipal corporations, and townships that pertain to matters that are expressly set forth or regulated under the bill. (Section 3.)

COMMENT

Existing 15 U.S.C. 7001 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
Reported, H. Civil & Commercial Law	06-23-05	p.	1423
Passed House (90-0)	08-02-05	pp.	1587-1588

h0104-ph-126.doc/kl