

Commerce, Insurance & Economic Development Task Force
Telecommunications & Information Technology Task Force
8/4/05 DRAFT (Telecom-IT Task Force):

8/5/05 DRAFT (CIED Task Force):

Breach of Personal Information Notification Act – VERSION I & II Combined
As amended and recommended by Joint Working Group, 8/3/05

NOTE: *This Act must first be recommended by the joint meeting of the Banking & Finance Subcommittee of the Commerce, Insurance & Economic Development Task Force, and the E-Commerce Subcommittee of the Telecommunications & Information Technology Task Force, on August 3, 2005 before being eligible for consideration by either full Task Force.*

Summary

This Act will help ensure that personal information residents of this state is protected by [providing procedures for notification of security breaches related to personal information and thereby](#) encouraging individuals and commercial entities, as defined in the bill, to provide reasonable security for unencrypted personal information. ~~In addition, this Act provides procedures for notification of security breaches related to personal information.~~

Model Legislation

Section 1. {Definitions}

As used in this Act:

1. "Breach of the security of a system" means the unauthorized access and acquisition of unencrypted [and unredacted](#) computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes or the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of this state.
 - a. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.
2. "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.
3. "Encrypted~~ion~~." ~~means The use of an algorithmic process to~~ transformation of data [through the use of an algorithmic process to](#) into a form in which there is a low probability of

assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.

4. "Financial institution" has the meaning given that term in section 6809(3) of title 15, United States Code.

4.5. "Individual" means a natural person.

5.6. a. "Personal information" means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are ~~not~~ neither encrypted nor redacted:

- a. Social Security number;
- b. Driver's license number or state identification card number issued in lieu of a driver's license; or
- c. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

b. The term does not include information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public.

6.7. "Notice" means:

- a. Written notice to the postal address in the records of the individual or entity;
- b. Telephone notice;
- c. Electronic notice, ~~if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Sec.7001 of Title 15 of the United States Code~~; or

d. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, or that the affected class of residents to be notified exceeds 100,000 persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in paragraphs a., b. or c. Substitute notice consists of any two of the following:

- i. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; and
- ii. Conspicuous posting of the notice on the Web site of the individual or the entity if the individual or the commercial entity maintains a Web site; and

iii. Notice to major statewide media.

7.8. "Redact:" ~~means~~ ~~The term includes, but is not limited to,~~ alteration or truncation of data such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the personal information.

Section 2. {Disclosure of Breach of Security of Computerized Personal Information by an Individual or Entity}

1. General rule.--An individual or entity 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 of the security of the system to any resident of this State whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this State. Except as provided in paragraph 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay.
2. Encrypted information.--An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this State.
3. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or is the entity reasonably believes was accessed and acquired by an unauthorized person.
4. Notice required by this Section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice required by ~~this Section e-chapter~~ this Section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.

Section 3. {Procedures Deemed in Compliance with Security Breach Requirements}

1. Information privacy or security policy.--An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and ~~that are is~~ consistent with the timing requirements of this Act shall be deemed to be in compliance with the notification requirements of this Act if it notifies ~~residents of this state subject persons~~ in accordance with its ~~procedures policies~~ in the event of a breach of security of the system.
2. Compliance with Federal requirements.
 - a. A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this Act.
 - b. An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this Act.

Section 4. {Violations}

1. A violation of this Act that results in injury or loss to residents of this State may be enforced by the Office of the Attorney General as an unfair trade practice pursuant to section ____.

2. Except as provided by paragraph 3, ~~T~~the Office of Attorney General shall have exclusive authority to bring action and may obtain either actual damages for a violation of this Act or a civil penalty not to exceed \$150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

3. A violation of this Act by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator.

Section 5. {Applicability}

This Act shall apply to the discovery or notification of a breach of the security of the system that occurs on or after the effective date of this section.

Section 6. {Effective Date} This Act shall take effect in 120 days after the date of enactment.

Section 7 {Preemption}.

This Act deals with subject matter that is of Statewide concern, and it is the intent of the Legislature that this Act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within this state regarding the matters expressly set forth in this Act.