

Commerce, Insurance & Economic Development Task Force
Telecommunications & Information Technology Task Force
8/04/05 Draft (Telecom-IT Task Force):
8/05/05 Draft (CIED Task Force):
Breach of Personal Information Notification Act – VERSION III

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 requires entities, government included, that do business in this state or who have customers in this state, to notify individuals within a reasonable period of time when there has been an unauthorized acquisition of personal information in paper, unencrypted or encrypted form.

Model Legislation

Section 1. {Definitions}

As used in this Act:

1. "Entity" means a person, other than an individual, that does any of the following:
 - a. Conducts business in this state and maintains personal information in the ordinary course of business;
 - b. Stores personal information in this state;
 - c. Maintains for a resident of this state a depository account, which means a certificate of deposit, demand, negotiated order of withdrawal, savings, share, time, or like account maintained with a bank, credit union, insurance company, savings bank, savings and loan association, securities broker or dealer or like organization. It does not include a safe deposit box or property deposited in a safe deposit box.
 - d. Lends money to a resident of this state;
 - e. The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the

constitution or any law, including the legislature and the courts;

f. A city, village, town or county.

2. "Personal Information" means any of the following information, if the information is accompanied by the name of the individual to whom the information pertains and is not publicly available:

- a. An individual's electronic mail address;
- b. The unique identifying driver number assigned to the individual by the department of transportation;
- c. An individual's social security number;
- d. An individual's employer or place of business
- e. An identification number assigned to an individual by his or her employer;
- f. The maiden name of the individual's mother
- g. The identifying number of a depository account of an individual;
- h. An individual's taxpayer identification number;
- i. An individual's deoxyribonucleic acid profile;
- j. Any of the following, if it can be used, alone or in conjunction with any access device, to obtain money, goods services, or any other thing of value or benefit, or if it can be used to initiate a transfer of funds:
 - i. An individual's code or account number;
 - ii. An individual's electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier;
 - iii. Any other means of account access.
- k. An individual's unique biometric data, including fingerprint, voice print, retina or iris image, or other unique physical representation;

- l. Any other information or data that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled;
 - m. Any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.
3. “Publicly available information” means any information that an entity reasonably believes is one of the following:
 - a. Information that is lawfully made widely available through the media.
 - b. Information that is lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.

Section 2. {Notice Required}

1. If an entity whose principal place of business is located in this state or an entity that stores personal information in this state knows that personal information in the entity’s possession has been obtained by a person whom the entity has not authorized to obtain that personal information, the entity shall make reasonable efforts to notify each individual who is subject of the personal information. The notice shall indicate that the entity knows of the unauthorized use of personal information pertaining to the individual.
2. If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been obtained by a person whom the entity has not authorized to obtain that personal information, the entity shall make reasonable efforts to notify each resident of this state who is subject of the personal information. The notice shall indicate that the entity knows of the unauthorized use of personal information pertaining to the individual.

- a. An entity shall provide the notice required within reasonable time, not to exceed 15 business days after the entity learns of the acquisition of personal information. A determination as to the reasonableness under this subsection shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.
- b. An entity shall provide the notice by mail or by method the entity has previously employed to communicate with the subject of the personal information. If the entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.

Section 3. {Violations}

1. Compliance with this section is not a defense to a claim in a civil action or proceeding.
2. Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of legal duty.

Section 4. {Delay of Notification}

If a law enforcement agency asks an entity not to provide a notice that is otherwise required for any period of time, the notification process shall begin at the end of that period of time.

Section 5. {Severability}

Section 6. {Effective Date}