PRINTER'S NO. 1169

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1023 Session of 2005

INTRODUCED BY PRESTON, FLICK, SHAPIRO, READSHAW, CRAHALLA, ROONEY, SAINATO, SOLOBAY, TANGRETTI, BLACKWELL, BOYD, CALTAGIRONE, GEORGE, GOOD, HALUSKA, HARRIS, HENNESSEY, HERSHEY, JAMES, JOSEPHS, KIRKLAND, LEACH, MAHER, MARKOSEK, McCALL, McGEEHAN, MUNDY, PALLONE, PETRONE, PISTELLA, STURLA, TIGUE, WALKO, WANSACZ, WHEATLEY AND YOUNGBLOOD, MARCH 16, 2005

REFERRED TO COMMITTEE ON JUDICIARY, MARCH 16, 2005

AN ACT

Providing for the notification of residents whose personal information data was or may have been disclosed due to a security system breach; and providing for penalties.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Short title.

This act shall be known and may be cited as the Breach of Personal Information Data Notification Act.

Section 2. Definitions.

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Breach of the security of the system." The unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the entity. Good faith acquisition of personal information by

an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure.

"Business." A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

"Customer." An individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

"Entity." A State agency or an individual or a business doing business in this Commonwealth.

"Individual." A natural person.

"Notice."

(1) Except as provided in paragraph (2), all of the following methods of notification:

(i) Notification to major Statewide media.

(ii) One of the following methods of notification:

(A) Written notice.

(B) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 701 of the Electronic Signatures in Global and National Commerce Act (Public Law 106-229, 15 U.S.C. § 7001).

(C) (I) Substitute notice, if the entity

demonstrates one of the following:

(a) The cost of providing notice would exceed $250,000.

(b) The affected class of subject persons to be notified exceeds $500,000.

(c) The entity does not have sufficient contact information.

(II) Substitute notice shall consist of all of the following:

(a) E-mail notice when the entity has an e-mail address for the subject persons.

(b) Conspicuous posting of the notice on the entity's Internet website, if the entity maintains one.

(2) Notwithstanding the provisions of paragraph (1), an entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise 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 subject persons in accordance with its policies in the event of a breach of security of the system.

"Personal information."

(1) 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 data elements are not encrypted:

(i) Social Security number.

(ii) Driver's license number or identification card number.

(iii) Account number, 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.

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

"Records." 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. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

"State agency." Any agency, board, commission, authority or department of the Commonwealth and the General Assembly.

Section 3. Disclosure of owned or licensed computerized data.

An 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 in the security of the data to any resident of this Commonwealth whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Except as provided in section 5 (relating to exception) or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the disclosure shall be made in the most expedient time possible and without unreasonable delay.

Section 4. Disclosure of maintained computerized data.

An entity that maintains computerized data that includes personal information that the entity 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 is reasonably believed to have been acquired by an unauthorized person.

Section 5. Exception.

The notification required by this act may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation.

Section 6. Violations.

A violation of this act shall be deemed to be a violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law.

Section 10. Applicability.

This act shall apply to the discovery or notification of a breach in the security of personal information data that occurs on or after the effective date of this section.

Section 11. Effective date.

This act shall take effect in 60 days.