PRIOR PRINTER'S NO. 2566 PRINTER'S NO. 2588

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1846 Session of 2017

INTRODUCED BY ELLIS, IRVIN, RABB, MILNE, PICKETT, BAKER, DAVIS, QUIGLEY, BOBACK, CHARLTON, O'NEILL, GROVE, DRISCOLL, THOMAS, MILLARD, JAMES, A. HARRIS, GODSHALL, KORTZ, C. QUINN, D. COSTA, TOEPEL, TALLMAN, KAMPF, HEFFLEY, WATSON, SCHWEYER AND DeLUCA, OCTOBER 13, 2017

AS REPORTED FROM COMMITTEE ON COMMERCE, HOUSE OF REPRESENTATIVES, AS AMENDED, OCTOBER 16, 2017

AN ACT

Amending the act of December 22, 2005 (P.L.474, No.94), entitled "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 imposing penalties," further providing for definitions and for notification of breach; providing for notification; further providing for notice exemption; ~~providing for safeguarding of personal information;~~ and further providing for civil relief. <--

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

Section 1. The definitions of "breach of the security of the system," "notice" and "personal information" in section 2 of the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, are amended and the section is amended by adding definitions to read:

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 access and acquisition of computerized data that materially compromises] loss, unauthorized access, acquisition or use of unencrypted data, encrypted data, the confidential process or key that is capable of compromising the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals [and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth]. 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 for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Bureau." The Bureau of Consumer Protection in the Office of Attorney General.

* * *

"Health insurance information." An individual's health insurance policy number or subscriber identification number, a unique identifier used by a health insurer to identify the individual or information in an individual's application and claims history, including appeals records.

* * *

"Medical information." Information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional.

"Notice." The term shall include notice of residents and notice of Commonwealth.

"Notice of Commonwealth." Written notice to the Director of

the Bureau of Consumer Protection of the Office of Attorney General.

"Notice of residents." [May be provided by any] For residents of this Commonwealth, any of the following methods of notification:

(1) Written notice to the last known home address for the individual.

(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.

(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.

(4) (i) Substitute notice, if the entity demonstrates one of the following:

(A) The cost of providing notice would exceed $100,000.

(B) The affected class of subject persons to be notified exceeds 175,000.

(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.

(C) Notification to major Statewide media.

"Personal information." Information that is under the control of an individual, is not otherwise generally available to the public through lawful means and is linked or linkable by the person to a specific individual or linked to a device that is associated with or routinely used by a specific individual, including:

~~(1) An individual's first name or first initial and last~~ <-- ~~name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:~~

~~(i) Social Security number.~~

~~(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.~~

~~(iii) Financial 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.~~

~~(1.1) Any of the following for an individual:~~

~~(i) A government-issued identification number, including a tax identification number and a passport number.~~

~~(ii) A postal address.~~

~~(iii) An e-mail address.~~

~~(iv) A telephone number.~~

~~(v) A fax number.~~

~~(vi) A debit or credit card number.~~

~~(vii) Medical information.~~

~~(viii) Health insurance information.~~

~~(ix) A biometric identifier, including a fingerprint or voice print.~~

~~(x) A unique persistent identifier, including:~~

~~(A) A number or alphanumeric string that uniquely identifies a networked device.~~

~~(B) An identification number or service account number, including a financial account number, credit card or debit card number, health account number or retail account number.~~

~~(C) A unique vehicle identifier, including a vehicle identification number or license plate number.~~

~~(D) A security code, access code or password that is necessary to access an individual's service account.~~

~~(xi) A unique identifier or other uniquely assigned or descriptive information about a personal computing or communication device.~~

~~(xii) Information that is collected, created, processed, used, disclosed, stored or otherwise maintained and linked or linkable by the person to any of the information enumerated under this paragraph.~~

(1) AN INDIVIDUAL'S FIRST NAME OR FIRST INITIAL AND LAST **<--** NAME IN COMBINATION WITH AND LINKED TO ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS WHEN EITHER THE NAME OR THE DATA ELEMENTS ARE NOT ENCRYPTED OR REDACTED:

(I) [SOCIAL SECURITY NUMBER.] IDENTIFICATION NUMBERS, SUCH AS:

(A) SOCIAL SECURITY NUMBER.

(B) DRIVER'S LICENSE NUMBER.

(C) STATE IDENTIFICATION CARD NUMBER ISSUED IN LIEU OF A DRIVER'S LICENSE.

(D) PASSPORT NUMBER.

(E) TAXPAYER IDENTIFICATION NUMBER.

(F) PATIENT IDENTIFICATION NUMBER.

(G) INSURANCE MEMBER NUMBER.

(H) EMPLOYEE IDENTIFICATION NUMBER.

(II) [DRIVER'S LICENSE NUMBER OR A STATE IDENTIFICATION CARD NUMBER ISSUED IN LIEU OF A DRIVER'S LICENSE.] OTHER ASSOCIATED NAMES, SUCH AS:

(A) MAIDEN NAME.

(B) MOTHER'S MAIDEN NAME.

(C) ALIAS.

(III) FINANCIAL ACCOUNT NUMBER, CREDIT OR DEBIT CARD NUMBER, ALONE OR IN COMBINATION WITH ANY REQUIRED EXPIRATION DATE, SECURITY CODE, ACCESS CODE OR PASSWORD THAT WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL ACCOUNT.

(IV) ELECTRONIC IDENTIFIER OR ROUTING CODE, IN COMBINATION WITH ANY REQUIRED SECURITY CODE, ACCESS CODE OR PASSWORD THAT WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL ACCOUNT.

(V) ELECTRONIC ACCOUNT INFORMATION, SUCH AS ACCOUNT NAME OR USER NAME.

(VI) INTERNET PROTOCOL (IP) OR MEDIA ACCESS CONTROL (MAC) ADDRESS OR OTHER HOST-SPECIFIC PERSISTENT STATIC IDENTIFIER THAT CONSISTENTLY LINKS TO A PARTICULAR INDIVIDUAL OR SMALL, WELL-DEFINED GROUP OF INDIVIDUALS.

(VII) BIOMETRIC DATA, SUCH AS GENETIC INFORMATION, A FINGERPRINT, FACIAL SCAN, RETINA OR IRIS IMAGE, VOICE SIGNATURE, X-RAY IMAGE OR OTHER UNIQUE PHYSICAL REPRESENTATION OR DIGITAL REPRESENTATION OF BIOMETRIC DATA.

(VIII) DATE OF BIRTH.

(IX) PLACE OF BIRTH.

(X) INSURANCE INFORMATION.

(XI) EMPLOYMENT INFORMATION.

(XII) EDUCATION INFORMATION.

(XIII) VEHICLE INFORMATION, SUCH AS:

(A) REGISTRATION NUMBER.

(B) TITLE NUMBER.

(XIV) CONTACT INFORMATION, SUCH AS:

(A) TELEPHONE NUMBER.

(B) ADDRESS.

(C) E-MAIL ADDRESS.

(XV) DIGITIZED OR OTHER ELECTRONIC SIGNATURE.

(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.

* * *

Section 2. Section 3(a) of the act is amended and the section is amended by adding subsections to read:

Section 3. Notification of breach.

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system [to any resident of this Commonwealth whose unencrypted and

unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person]. Except as provided in section 4 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 notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

* * *

(d) Notice to residents of this Commonwealth.--

(1) Notification must be in plain language.

(2) Notice of the breach of the security of the system under this section shall be made to the affected residents of this Commonwealth and must include the following:

(i) The date, estimated date or date range of the breach of the security of the system.

(ii) Whether the notification was delayed as a result of a law enforcement investigation.

(iii) A list of types of information that were or are believed to have been subject to the breach of the security of the system.

(iv) A general description of the breach of the security of the system.

(v) Toll-free telephone numbers and addresses of consumer reporting agencies if the breach of the security of the system exposed a Social Security number or an identification card number.

(vi) The name and contact information of the

reporting agency that was notified under section 5.

(3) The entity providing notice under this subsection may include information about what the entity has done to protect affected individuals and offer advice on what steps affected individuals may take to protect their information and what steps the individual whose information has been breached may take to protect himself or herself.

(4) Notice under this subsection shall be made within ~~30~~ 45 days of learning of the breach of the security of the system. <-- <--

(e) Notice to Attorney General.--

(1) Notice of the breach of the security of the system under this section shall be made to the bureau.

(2) Notice under this subsection must include the following:

(i) The nature of the breach of the security of the system.

(ii) The number of residents of this Commonwealth affected by the breach of the security of the system.

(iii) Steps taken by the entity relating to the breach of the security of the system.

(3) Notice under this subsection shall be made within 30 days of the breach of the security of the system.

(f) State agencies.--If a State agency is the subject of a breach of security of the system, the State agency must provide notice of the breach of security of the system required under subsection (a) without unreasonable delay following discovery of the breach. A State agency under the Governor's jurisdiction shall provide notice of a breach of the security of the system to the Governor's Office of Administration without unreasonable

delay. Notification under this subsection shall occur notwithstanding the procedures and policies under section 7.

(g) Counties, school districts and municipalities.--A county, school district or municipality shall provide notice to the district attorney in the county in which the breach occurred of a breach of the security of the system required under subsection (a) without unreasonable delay following discovery of the breach. Notification under this subsection shall occur notwithstanding the procedures and policies under section 7.

Section 3. The act is amended by adding a section to read:

Section 5.1. Notification.

When an entity provides notification under this act, the entity shall also notify, without unreasonable delay, the bureau of the timing, distribution and number of notices and any other information as required by the bureau.

Section 4. Section 7(b) of the act is amended by adding a paragraph to read:

Section 7. Notice exemption.

* * *

(b) Compliance with Federal requirements.--

* * *

(3) If an entity does not have a Federal or state notification rule, regulation, procedure or guideline in effect, the entity must comply with this act.

~~Section 5. The act is amended by adding a section to read:~~ <--

~~Section 7.1. Safeguarding of personal information.~~

~~(a) Duty. Any entity in possession of personal information of another person shall safeguard the data, computer files or documents containing the information from misuse by third parties and shall destroy, erase or make unreadable such data,~~

computer files or documents prior to disposal.

(b) Policy.--The entity shall develop a policy to govern the proper storage of data which includes personally identifiable information. The policy shall address identifying, collecting, maintaining, displaying and transferring personally identifiable information, using personally identifiable information in test environments, remediating personally identifiable information stored on legacy systems and other relevant issues. A goal of the policy shall be to reduce the risk of future breaches of security of the system.

(c) Privacy protection policy.--An entity that collects personal information in the course of business shall create a privacy protection policy, which shall be published or publicly displayed, including posting on an Internet web page. The policy shall protect the confidentiality of the personal information, prohibit unlawful disclosure of personal information and limit access to personal information. This subsection shall not apply to a Commonwealth agency or a political subdivision.

(d) Disposal policy.--

(1) When disposing of records, each entity shall meet the following minimum standards for proper disposal of records containing personal information:

(i) Paper records containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed.

(ii) Electronic records and other nonpaper records containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

(2) An entity disposing of personal information may contract with a third party to dispose of personal information in accordance with this section. A third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

(e) Unfair methods of competition and unfair or deceptive acts or practices.--The following shall be considered unfair methods of competition and unfair or deceptive acts or practices by an entity that collects or possesses personal information:

(1) Failing to create a storage policy as described under subsection (b).

(2) Failing to create, publish or publicly display or comply with a privacy protection policy as described under subsection (c).

(3) Failing to dispose of records in a manner described under subsection (d).

(4) Failing to provide consumers with opt-out consent prior to the entity using, disclosing or permitting a third party to have access to personal information of consumers or failing to provide consumer with a means to withdraw a previous consent.

(5) Refusing to provide service to consumers who exercise their right to opt out of an entity using, disclosing or permitting a third party from having access to their personal information.

(6) Failing to reasonably safeguard or protect personal

~~information, maintained by an entity or a vendor, from a breach of the security of the system.~~

Section ~~6~~ 5. Section 8 of the act is amended to read: <--

Section 8. Civil relief.

A violation of this act shall be deemed to be an unfair method of competition and an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

Section ~~7~~ 6. This act shall take effect in 60 days. <--