PRINTER'S NO. 1379

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 955 Session of 2019

INTRODUCED BY YAW, COLLETT, MASTRIANO AND YUDICHAK, NOVEMBER 15, 2019

REFERRED TO COMMUNICATIONS AND TECHNOLOGY, NOVEMBER 15, 2019

AN ACT

Requiring certain entities to provide notification of breach of personal information; and providing for a cause of action.

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 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:

"Access device." A card issued by a financial institution that contains a magnetic strip, microprocessor chip or other means for storage of information. The term includes a credit card, debit card or stored value card.

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal

information maintained by an 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 a resident of this Commonwealth. The term does not include good faith acquisition of personal information by an employee or agent of an entity for the purposes of the entity 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.

"Business." A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit. The term includes 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 also includes an entity that destroys records.

"Card security code." The three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic strip of an access device that is used to validate access device information during the authorization process.

"Encryption." The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"Entity." A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

"Financial institution." An office of a bank, bank and trust, trust company with banking powers, savings bank,

industrial loan company, savings association, credit union or regulated lender.

"Identity theft." The possession and use, through any means, by a person of identifying information of an individual without the consent of the individual to further an unlawful purpose.

"Magnetic strip data." Data contained in a magnetic strip of an access device.

"Microprocessor chip data." Data contained in a microprocessor chip of an access device.

"Notice." Any of the following methods of notification:

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

(2) Telephonic notice to a customer if:

(i) the customer can be reasonably expected to receive the notice;

(ii) the notice is given in a clear and conspicuous manner;

(iii) the notice describes the incident in general terms;

(iv) the notice verifies personal information;

(v) the notice does not require the customer to provide personal information; and

(vi) the customer is provided with a telephone number to call or a publicly accessible Internet website to visit for further information or assistance.

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

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

(i) the cost of providing notice would exceed $100,000;

(ii) the affected class of subject individuals to be notified exceeds 175,000; or

(iii) the entity does not have sufficient contact information.

(5) All of the following apply:

(i) There is e-mail notice, when the entity has an e-mail address for the subject individuals.

(ii) There is a conspicuous posting of the notice on the entity's publicly accessible Internet website, if the entity maintains one.

(iii) The notification is provided to major Statewide media.

"Personal information." 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:

(1) Social Security number.

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

(3) Financial account number, credit card number 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.

(4) Passport number.

(5) A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

(6) Medical history, medical treatment by a health care

professional, diagnosis of mental or physical condition by a health care professional or deoxyribonucleic acid profile.

(7) Health insurance policy number, subscriber identification number or any other unique identifier used by a health insurer to identify the individual.

(8) Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes.

(9) The individual's taxpayer identification number.

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

"PIN." A personal identification code that identifies the cardholder.

"PIN verification code number." Data used to verify cardholder identity when a PIN is used in a transaction.

"Records." 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.

"Redact." 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 data.

"Service provider." A person or entity that stores,

processes or transmits access device data on behalf of another person or entity.

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

Section 3. Notification of breach.

(a) Duty to provide.--

(1) An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of a breach of the security of the system following discovery of the breach of the security of the system to a 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.

(2) 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.

(3) For the purpose of this subsection, a resident of this Commonwealth may be determined to be an individual whose principal mailing address as reflected in the computerized data that is maintained, stored or managed by the entity is in this Commonwealth.

(b) Encrypted information.--An entity shall provide notice of the breach if:

(1) encrypted information is accessed and acquired in an unencrypted form;

(2) the security breach is linked to a breach of the security of the encryption; or

(3) the security breach is committed by a person with

access to or who otherwise learns of the encryption key.

(c) Vendor notification.--

(1) A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of a breach of the security of the system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data.

(2) The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

Section 4. Exceptions.

The notification required by this act may be delayed for up to three days if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation.

Section 5. Notification to consumer reporting agencies.

When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.

Section 6. Preemption.

This act relates to subject matter that is of Statewide concern, and it is the intent of the General Assembly 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 Commonwealth relating to the provisions of this act.

Section 7. Notice exemption.

(a) 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 is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if the entity notifies subject individuals in accordance with the entity's policies in the event of a breach of security of the system.

(b) Compliance with Federal requirements.--

(1) 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.

(2) An entity that complies with the notification requirements or procedures under the rules, regulations, procedures or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this act.

Section 8. Civil relief.

(a) Remedies for residents.--A resident of this Commonwealth who is adversely affected by a violation of this act, in addition to and cumulative of all other rights and remedies available at law, may bring an action to:

(1) Enjoin further violations of this act.

(2) Recover the greater of actual damages or $5,000 for each separate violation of this act.

(b) Attorney General.--The Attorney General may bring an action against a person who violates this act to:

(1) Enjoin further violation of this act.

(2) Recover a civil penalty not to exceed $10,000 per violation.

(c) Limitation period.--An action under this section must be brought within three years after the violation is discovered or by the exercise of reasonable diligence should have been discovered, whichever is earlier.

(d) Repeated violations.--In an action under this section, the court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this section if the court determines that the defendant has engaged in a pattern and practice of violating this section.

(e) Attorney fees and costs.--A prevailing plaintiff in an action under this section shall be entitled to recover the plaintiff's reasonable attorney fees and costs.

(f) Arbitration.--The rights of residents of this Commonwealth and their access to the Commonwealth's courts are in addition to and are not barred by any arbitration provision in a contract between a resident of this Commonwealth and a business.

(g) Violations.--For the purpose of this section, multiple violations of this act resulting from a single action or act shall constitute one violation.

Section 9. Information security.

(a) Security or identification information.--An entity that maintains, stores or manages computerized data that includes personal information shall take reasonable measures, consistent with the nature and size of the entity, to secure the system and unredacted personal information of residents of this Commonwealth.

(b) Liability.--If there is a breach of security of the system of a person or entity that has violated this section, or the person's or entity's service provider, the person or entity shall compensate the individual affected by the breach for identity theft and fraudulent charges in the amount of $5,000 for each separate violation of this act or the actual damages incurred, whichever is greater.

Section 10. Access devices and breach of security.

(a) Security or identification information and retention prohibited.--

(1) No person or entity conducting business in this Commonwealth that accepts an access device in connection with a transaction may retain the card's security code data, the PIN verification code number or the full contents of any tract magnetic strip data subsequent to the authorization of the transaction or, in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

(2) A person or entity is in violation of this section if the entity's service provider retains the data subsequent to the authorization of the transaction or, in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

(b) Liability.--If there is a breach of the security of the system of a person or entity that has violated this act, or of the person's or entity's service provider, the person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of the entity's

cardholders or to continue to provide services to cardholders, including any cost incurred in connection with:

(1) The cancellation or reissuance of any access device affected by the breach.

(2) The closure of a deposit, transaction, share draft or other account affected by the breach and any action to stop a payment or block a transaction with respect to the account.

(3) The opening or reopening of a deposit, transaction, share draft or other account affected by the breach.

(4) A refund or credit made to a cardholder to cover the cost of an unauthorized transaction relating to the breach.

(5) The notification of cardholders affected by the breach.

(c) Recovery of costs.--

(1) The financial institution may recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this act.

(2) Costs do not include an amount recovered from a credit card company by a financial institution.

(3) The remedies under this subsection are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

Section 11. 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 12. Effective date.

This act shall take effect in 60 days.