SPONSOR: Rep. Baumbach & Rep. Bolden & Rep. Hudson & Sen. Sokola & Sen. Lopez & Sen. Pettyjohn
Reps. Bennett, Brady, Kowalko, Miro, Viola; Sen. Hansen

HOUSE OF REPRESENTATIVES
149th GENERAL ASSEMBLY

HOUSE BILL NO. 180

AN ACT TO AMEND TITLE 6 OF THE DELAWARE CODE RELATING TO BREACHES OF SECURITY INVOLVING PERSONAL INFORMATION.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

Section 1. Amend Chapter 12B, Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline and renumbering accordingly as follows:

§ 12B-100. Protection of personal information.

Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized access to or acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.

§ 12B-101. Definitions.

For purposes of this chapter:

(1) ~~"Breach of the security of the system" means the~~ "Breach of security" means as follows:

~~the~~ a. The unauthorized acquisition or disclosure of ~~unencrypted~~ electronic or paper files, media, databases, or other ~~computerized~~ data that compromises the security, confidentiality, or integrity of personal ~~information maintained by an individual or a commercial entity.~~ information. Good faith acquisition of personal information by an employee or agent of ~~an individual or a commercial entity~~ any person for the purposes of ~~the individual or the commercial entity~~ such person is not a breach of ~~the security of the system,~~ security, provided that the personal information is not used or subject to further unauthorized ~~disclosure;~~ disclosure.

b. The intentional unauthorized access to, use, or modification of personal information.

c. The unauthorized access to or the acquisition, or disclosure of electronic or paper files, media, databases, or other data is not a breach of security to the extent that such electronic or paper files, media, databases, or other data are encrypted, unless such unauthorized access, acquisition, or disclosure includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the

encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.

~~(2) "Commercial entity" includes corporations, business trusts, estates, trusts, 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;~~

( ) "Encrypted" means electronic or paper files, media, databases, or other data that is rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.

( ) "Encryption key" means the confidential key or process designed to render the encrypted data useable, readable, and decipherable.

(3) "Notice" ~~means:~~ means any of the following:

a. Written ~~notice;~~ notice.

b. Telephonic ~~notice;~~ notice.

c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States ~~Code; or~~ Code, but electronic notice is not permitted if the breach involves a username or email address, in combination with a password or security question and answer that would permit access to the online account that would receive the notice.

d. Substitute notice, if the ~~individual or the commercial entity~~ person required to provide notice under this chapter demonstrates that the cost of providing notice will exceed $75,000, or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the ~~individual or the commercial entity~~ person does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

1. ~~E-mail~~ Electronic notice if the ~~individual or the commercial entity~~ person has e-mail addresses for the members of the affected class of Delaware ~~residents; and~~ residents.

2. Conspicuous posting of the notice on the web site page of the ~~individual or the commercial entity~~ person if the ~~individual or the commercial entity~~ person maintains ~~one; and~~ one.

3. Notice to major statewide ~~media.~~ media, including newspapers, radio, and television and publication on the major social media platforms of the person providing notice.

(4)a. "Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to ~~the resident, when either the name or the data elements are not encrypted:~~ that individual:

~~a.~~ 1. Social Security ~~number;~~ number.

~~b.~~ 2. Driver's license number or ~~Delaware Identification Card number; or~~ state or federal identification card number.

~~c.~~ 3. Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

4. Passport number.

5. Shared secrets or security tokens that are known to be used for data-based authentication.

6. A username or email address, in combination with a password or security question and answer that would permit access to an online account.

7. A marriage certificate or marriage certificate number.

8. Full date of birth or birth certificate.

9. Medical history, mental or physical condition, medical treatment, or diagnosis by a health care professional or deoxyribonucleic acid profile.

10. Health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the person or information related to a person's application or claims history.

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

12. An individual taxpayer identification number.

13. Information or data collected through the use or operation of an automated license plate recognition system.

14. Unique electronic identification number or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

15. An individual's digital or electronic signature.

b. ~~The term "personal~~ "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government ~~records;~~ records or widely-distributed media.

§ 12B-102. Disclosure of breach of security; notice. ~~security of computerized personal information by an individual or a commercial entity.~~

~~(a) An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.~~

(a) Any person who conducts business in this State and who owns or licenses electronic or paper files, media, databases, or other data that includes personal information shall provide notice of any breach of security following the discovery of the breach of security to any resident of this State whose personal information was breached or is reasonably believed to have been breached, unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

(b) ~~An individual or a commercial entity~~ A person that maintains ~~computerized~~ electronic or paper files, media, databases, or other data that includes personal information that the ~~individual or the commercial entity~~ person does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of ~~the~~ security ~~of the system~~ immediately following discovery of ~~a breach, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur. Cooperation~~ the breach of security. For purposes of this subsection, "cooperation" includes sharing with the owner or licensee information relevant to the breach.

(c) Notice required by § 12B-102(a) of this chapter ~~may be delayed~~ must be made without unreasonable delay but not later than 60 days after the discovery of the breach, unless a shorter time is required under federal law or if a ~~law-enforcement~~ law enforcement agency determines that the notice will impede a criminal investigation and such law enforcement agency has made a request of the person that the notice be delayed. ~~Notice required by this chapter must be made in good faith, without unreasonable delay and as soon as possible after the law-enforcement agency determines that notification will no longer impede the investigation.~~ Any such delayed notice must be made after such law enforcement agency determines that notice will not compromise the criminal investigation and so notifies the person of such determination.

(d) If the affected class of Delaware residents to be notified exceeds 500 residents, the person required to provide notice shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General.

(e) If the breach of security includes a complete social security number, the person shall offer to each resident, whose personal information, including social security number, was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such services must be provided at no cost to such resident for a period of not less than 1 year. Such person shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on such resident's credit file. Such services are not required if, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

(f) The Director of Consumer Protection of the Department of Justice shall promulgate regulations setting forth the required form and content of a notice under this chapter.

Section 2. Amend § 12B-103, Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows:

§ 12B-103. Procedures deemed in compliance with security breach requirements.

(a) Under this chapter, ~~an individual or a commercial entity~~ a person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the ~~individual or the commercial entity~~ person notifies affected Delaware residents in accordance with its policies in the event of a breach of ~~security of the system.~~security.

(b) Under this chapter, ~~an individual or a commercial entity~~ a person that is regulated by state or federal law and that maintains procedures for a breach of ~~the~~ security ~~of the system~~ pursuant to the laws, rules, regulations, ~~guidances,~~guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the ~~individual or the commercial entity~~ person notifies affected Delaware residents in accordance with the maintained procedures when a breach occurs.

Section 3. Amend § 12B-104, Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows:

§ 12B-104. Violations.

141 (a) Pursuant to the enforcement duties and powers of the Director of Consumer Protection ~~Division~~ of the

142 Department of Justice under Chapter 25 of Title 29, the Attorney General may bring an action in law or equity to address

143 the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to

144 recover direct economic damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do

145 not relieve ~~an individual or a commercial entity~~ a person subject to this chapter from compliance with all other applicable

146 provisions of law.

147 (b) Any person harmed by a violation of § 12B-102 of this title may bring an action for recovery of damages.

148 (c) Nothing in this chapter may be construed to nullify or impair any right which a person may have at common

149 law, by statute, or otherwise.

SYNOPSIS

This Act amends Chapter 12B of Title 6 to update Delaware's law regarding computer security breaches by doing the following:

1. Creating a requirement that any person who conducts business in Delaware and maintains personal information must safeguard that information.
2. Updating the definition of breach of security by including the unauthorized access, use, modification, or disclosure of personal information and the information that is included in the definition of personal information.
3. Adding definitions for encryption.
4. Creating a "safe harbor" if the data included in an breach is encrypted or protected by an encryption key that prevents the data from being read or used.
5. Strengthening the consumer protections when a security breach is discovered including requiring that the entity that experienced the breach provide identity theft protection services if Social Security Numbers were included in the information breached.

This Act also makes technical corrections to conform to the standards of the Delaware Legislative Drafting Manual, including the use of the term "person" to mean both an individual and an artificial entity.