AMENDED IN ASSEMBLY APRIL 10, 2007

CALIFORNIA LEGISLATURE—2007–08 REGULAR SESSION

ASSEMBLY BILL No. 779

Introduced by Assembly Member Jones

February 22, 2007

An act to ~~amend Section 1798.82 of~~ *add Section 1724 to, and to repeal and amend Sections 1798.29 and 1798.82 of,* the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

AB 779, as amended, Jones. Personal information: ~~computerized data: breaches~~ *state agencies and businesses*.

(1) Existing law imposes specified duties upon certain persons or businesses that conduct business in California to, among other things, take reasonable steps to destroy customer records, implement and maintain reasonable security measures, disclose a breach of computerized data, and, upon request, provide specified information to a customer in relation to the disclosure of personal information to 3rd parties. For a violation of any of the above-described provisions, existing law allows an injured customer to institute a civil action to recover damages or for injunctive relief.

This bill would subject a retail seller to the above-described provisions. The bill would also prohibit a retail seller from retaining personal information for longer than 90 days after the date of an original transaction or as specified.

~~Existing~~

(2) Existing law requires any *state agency, or a* person or business that conducts business in California, ~~and~~ that owns or licenses computerized data that includes personal information, *as defined*, to

disclose any breach of ~~that data~~ *the security of that data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person*.

This bill would ~~make technical, nonsubstantive changes to that provision~~ *require that notification to include, among other things, a description of the categories of personal information that was, or may have been, acquired, a toll-free telephone number or electronic mail address an individual may use to contact the agency or person or business, and the telephone numbers and addresses of the major credit reporting agencies, and would require a copy to be provided to the Office of Privacy Protection. The bill would also allow a person or business subject to the above-described provisions to, if applicable, be reimbursed by whomever maintains the personal information for all reasonable costs of providing notice regarding a breach. The bill would also repeal duplicative provisions of law*.

Vote: majority. Appropriation: no. Fiscal committee: ~~no~~ *yes*. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1724 is added to the Civil Code, to read:

1724. (a) For purposes of this section, "personal information" has the same meaning as in subdivision (e) of Section 1798.80.

(b) Any retail seller that sells goods or services to any resident of California that collects or maintains personal information for any purpose shall be subject to the provisions of Title 1.81 (commencing with Section 1798.80) of Part 4.

(c) A retail seller that sells goods or services to any resident of California shall not retain personal information for longer than 90 days after the date of the original transaction, or the period of time during which goods may be returned for a refund or exchange, whichever is shorter.

SEC. 2. Section 1798.29 of the Civil Code, as added by Section 2 of Chapter 915 of the Statutes of 2002, is repealed.

~~1798.29. (a) Any agency 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 California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The~~

~~disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.~~

~~(b) Any agency that maintains computerized data that includes personal information that the agency 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.~~

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

~~(d) For purposes of this section, "breach of the security of the system" means unauthorized aquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.~~

~~(e) For purposes of this section, "personal information" means 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 the data elements are not encrypted:~~

~~(1) Social security number.~~

~~(2) Driver's license number or California Identification Card number.~~

~~(3) 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.~~

~~(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.~~

~~(g) For purposes of this section, "notice" may be provided by one of the following methods:~~

~~(1) Written notice.~~

~~(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.~~

~~(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:~~

~~(A) E-mail notice when the agency has an e-mail address for the subject persons.~~

~~(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.~~

~~(C) Notification to major statewide media.~~

~~(h) Notwithstanding subdivision (g), an agency 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 part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.~~

SEC. 3. Section 1798.29 of the Civil Code, as added by Section 2 of Chapter 1054 of the Statutes of 2002, is amended to read:

1798.29. (a) Any agency 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 California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) *(1)* Any agency that maintains computerized data that includes personal information that the agency 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.

(2) A copy of the notice sent pursuant to this section shall be provided to the Office of Privacy Protection. Notification pursuant to this section shall be written in plain English and shall include, at a minimum, all of the following:

(A) The date of the notice.

(B) The name of the agency that maintained the computerized data at the time of the breach.

(C) The date on which the breach occurred.

(D) A description of the categories of personal information that was, or is reasonably believed to have been, acquired by an unauthorized person.

(E) A toll-free telephone number or, if the primary method used by the agency to communicate with the individual is by electronic means, an electronic mail address that the individual may use to contact the agency, so that the individual may learn what types of personal information the agency maintained about that individual.

(F) The toll-free telephone numbers and addresses for the major credit reporting agencies.

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

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means 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 the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California ~~Identification Card~~ *identification card* number.

(3) 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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

(B) Conspicuous posting of the notice on the agency's *Internet* Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency 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 part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 4. Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 915 of the Statutes of 2002, is repealed.

~~1798.82. (a) Any person or business that conducts business in California, and 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 California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The~~

~~disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.~~

~~(b) Any person or business that maintains computerized data that includes personal information that the person or business 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.~~

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

~~(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.~~

~~(e) For purposes of this section, "personal information" means 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 the data elements are not encrypted:~~

~~(1) Social security number.~~

~~(2) Driver's license number or California Identification Card number.~~

~~(3) 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.~~

~~(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.~~

~~(g) For purposes of this section, "notice" may be provided by one of the following methods:~~

~~(1) Written notice.~~

~~(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.~~

~~(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:~~

~~(A) E-mail notice when the person or business has an e-mail address for the subject persons.~~

~~(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.~~

~~(C) Notification to major statewide media.~~

~~(h) Notwithstanding subdivision (g), a person or business 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 part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.~~

~~SECTION 1.~~

SEC. 5. Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 1054 of the Statutes of 2002, is amended to read:

1798.82. (a) Any person or business that conducts business in California, and 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 California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) *(1)* Any person or business ~~maintaining~~ *that maintains* computerized data that includes personal information that the person or business 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.

(2) A copy of the notice sent pursuant to this section shall be provided to the Office of Privacy Protection. Notification pursuant to this section shall be written in plain English and shall include, at a minimum, all of the following:

(A) The date of the notice.

(B) The name of the person or business that maintained the computerized data at the time of the breach.

(C) The date on which the breach occurred.

(D) A description of the categories of personal information that was, or is reasonably believed to have been, acquired by an unauthorized person.

(E) A toll-free telephone number or, if the primary method used by the person or business to communicate with the individual is by electronic means, an electronic mail address that the individual may use to contact the person or business or their agent, so that the individual may learn what types of personal information the person or business maintained about that individual.

(F) The toll-free telephone numbers and addresses for the major credit reporting agencies.

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

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of ~~unencrypted~~ computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California ~~Identification Card~~ *identification card* number.

(3) 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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the *Internet* Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business 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 part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(i) If notice is required to be provided pursuant to this section, the owner or licensee of the personal information shall be entitled to reimbursement from the person or business that maintains the computerized data for all reasonable and actual costs of providing notice to consumers regarding the breach of the security of the system as required by this section.

O