SB 46 (Corbett) – Personal Information: Privacy

Introduced December 14, 2012, Amended April 15, 2013

This bill would expand the scope of "personal information" subject to existing security breach disclosure requirements to include a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Existing law requires any state agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information as defined, to disclose any security breach concerning that data to any California resident whose unencrypted personal information was, or is believed to have been, acquired by an unauthorized person. Personal information covered by existing disclosure requirements includes an individual's first name and last name, or first initial and last name, when acquired in combination with, among other things, a social security number, driver's license or California Identification Card number, financial account number, or medical information.

Background:

In 2003, California's first-in-the nation security breach notification law went into effect. (See Civ. Code Secs. 1798.29(a), 1798.82(a).) Since that time, all but four states have enacted similar security breach notification laws, and governments around the world are considering enacting such laws. California's security breach notification statute requires state agencies and businesses to notify residents when the security of their personal information, as defined, is breached. That notification ensures that residents are aware of the breach and allows them to take appropriate actions to mitigate or prevent potential financial losses due to fraudulent activity, as well as to limit the potential dissemination of personal information.

A July 12, 2012, New York Times article entitled "Breach Extends Beyond Yahoo to Gmail, Hotmail, AOL Users," chronicled an example of a recent security breach that likely involved the personal information of California consumers. That article reported: Another month, another major security breach. Yahoo confirmed Thursday that about 400,000 user names and passwords to Yahoo and other companies were stolen on Wednesday.

A group of hackers, known as the D33D Company, posted online the user names and passwords for what appeared to be 453,492 accounts belonging to Yahoo, and also Gmail, AOL, Hotmail, Comcast, MSN, SBC Global, Verizon, BellSouth and Live.com users.

The hackers wrote a brief footnote to the data dump, which has since been taken offline: "We hope that the parties responsible for managing the security of this subdomain will take this as a wake-up call, and not as a threat."

The breach comes just one month after millions of user passwords for LinkedIn, the online social network for professionals, were exposed by hackers who breached its systems. The breaches highlight the ease with which hackers are able to infiltrate

systems, even at some of the most widely used and sophisticated technology companies.

The California Attorney General notes that "with 12.6 million victims in 2012, including over 1 million Californians, identity theft continues to be a significant crime." The Attorney General's specialized eCrime Unit finds, along with other law enforcement agencies, that increasingly "criminals are targeting websites with inadequate security, including some social media websites, to harvest email addresses, user names, and passwords," and "because most people do not use unique passwords for each of their accounts, acquiring the information on one account can give a thief access to many different accounts."

Responding to the increasing frequency of this type of security breach, this bill would expand the coverage of California's security breach notification law by specifically including user names and email addresses, when compromised in conjunction with passwords and security questions and answers.

Existing law:

- Requires any agency, person, or business that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Secs.1798.29(a) and (c) and 1798.82(a) and (c).)

- Requires any agency, person, or business that maintains computerized data that includes personal information that the agency, person, or business does not own to notify the owner or licensee of the information of any security breach immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code Secs. 1798.29(b) and 1798.82(b).)

- Defines "personal information," for purposes of the breach notification statute, to include the 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: social security number; driver's license number or California Identification Card number; 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; medical information; or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code Secs. 1798.29(g) and (h) and 1798.82(h) and (i))

AMENDED IN SENATE APRIL 15, 2013

SENATE BILL No. 46

Introduced by Senator Corbett

December 14, 2012

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 46, as amended, Corbett. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines "personal information" for these purposes, to include an individual's first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver's license numbers, financial accounts, and medical information.

This bill would revise certain data elements included within the definition of personal information, by adding certain information ~~relating to an account other than a financial~~ *that would permit access to an online* account.

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

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

SECTION 1. Section 1798.29 of the Civil Code 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) 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) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range

within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) 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.

(g) For purposes of this section, "personal information" means ~~an~~ *either of the following:*

(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 the data elements are not encrypted:

~~(1)~~

(A) Social security number.

~~(2)~~

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

~~(3)~~

(C) 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.

~~(4)~~

(D) Medical information.

~~(5)~~

(E) Health insurance information.

~~(6) Password, user name,~~

(2) A user name or email address, in combination with a password or security question and answer ~~for an account other than a financial~~ *that would permit access to an online* account.

(h) (1) 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.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) 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~~ *Email* notice when the agency has an ~~e-mail~~ *email* 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 and the Office of Information Security within the California Technology Agency.

(j) Notwithstanding subdivision (i), 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. 2. Section 1798.82 of the Civil Code 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) 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) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) 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.

(h) For purposes of this section, "personal information" means ~~an~~ *either of the following:*

(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 the data elements are not encrypted:

~~(1)~~

(A) Social security number.

~~(2)~~

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

~~(3)~~

(C) 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.

~~(4)~~

(D) Medical information.

~~(5)~~

(E) Health insurance information.

~~(6) Password, user name~~

(2) A user name or email address, in combination with a password or security question and answer ~~for an account other than a financial~~ *that would permit access to an online* account.

(i) (1) 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.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(j) 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~~ *Email* notice when the person or business has an ~~e-mail~~ *email* 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 and the Office of Privacy Protection within the State and Consumer Services Agency.

(k) Notwithstanding subdivision (j), 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.

O