

AMENDED IN ASSEMBLY MARCH 28, 2014

CALIFORNIA LEGISLATURE—2013–14 REGULAR SESSION

ASSEMBLY BILL

No. 1710

Introduced by Assembly Members Dickinson and Wieckowski

February 13, 2014

An act to amend ~~Section~~ *Sections 1798.81.5, 1798.82, 1798.84, and 1798.85* of, and to add *Sections 1724.4 and 1724.6* to, the Civil Code, relating to personal information privacy.

LEGISLATIVE COUNSEL'S DIGEST

AB 1710, as amended, Dickinson. Personal information: privacy.

Existing law requires a person or business conducting business in California that owns or licenses computerized data that includes personal information, as defined, to disclose, as specified, a breach of the security of the system or data 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.

~~This bill would make nonsubstantive, technical changes to these provisions.~~

This bill would instead require a person or business conducting business in California that owns or licenses computerized or noncomputerized data that contains personal information to disclose, as specified, a breach of the security of the system or data following discovery or notification of the security breach to any California resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. If the person or business was the source of the breach, the bill would require the person or business to offer to provide appropriate identity theft prevention and

mitigation services to the affected person at no cost for not less than 24 months if the breach exposed or may have exposed specified personal information. The bill would also require a person or business that maintains but does not own the data to notify the persons affected within 15 days of the breach using specified methods.

This bill would prohibit a person or business that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device, from storing, retaining, sending, or failing to limit access to payment-related data, as defined, retaining a primary account number, or storing sensitive authentication data subsequent to an authorization, as specified, unless a specified exception applies. The bill would make a person or business liable for the reimbursement of all reasonable and actual costs of providing notice of a breach of the security of a system or data following discovery or notification of the security breach to any California resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person, and for the reasonable and actual cost of card replacement as a result of a breach, to the owner or licensee of the information. The bill would authorize this liability to be excused, in whole or in part, if the person or business, can demonstrate compliance with specified provisions at the time of the breach.

Existing law requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

This bill would expand these provisions to businesses that own, license, or maintain personal information about a California resident, as specified.

Existing law authorizes any customer injured by a violation of specified provisions relating to customer records to institute a civil action to recover damages and penalties, as specified.

This bill would, in addition to any other available remedies, authorize a public prosecutor to bring an action to recover a civil penalty not exceeding \$500, or for a willful, intentional, or reckless violation not exceeding \$3,000, per violation.

Existing law prohibits a person or entity, with specified exceptions, from publicly posting or displaying an individual's social security number or doing certain other acts that might compromise the security

of an individual’s social security number, unless otherwise required by federal or state law.

This bill would also prohibit the sale, advertisement for sale, or offer to sell of an individual’s social security number. The bill would, in addition to any other available remedies for a violation of these provisions, authorize a public prosecutor to bring an action to recover a civil penalty not exceeding \$500 per violation.

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

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

- 1 SECTION 1. *Section 1724.4 is added to the Civil Code, to read:*
- 2 1724.4. (a) *In addition to being subject to the provisions of*
- 3 *Title 1.81 (commencing with Section 1798.80) of Part 4, a person*
- 4 *or business that sells goods or services to any resident of California*
- 5 *and accepts as payment a credit card, debit card, or other payment*
- 6 *device shall not do any of the following:*
- 7 (1) *Store payment-related data, unless the person or business*
- 8 *complies with both of the following:*
- 9 (A) *The person or business has a payment data retention and*
- 10 *disposal policy that limits the amount of payment-related data and*
- 11 *the time that data is retained to only the amount and time required*
- 12 *for business, legal, or regulatory purposes as explicitly documented*
- 13 *in the policy.*
- 14 (B) *The person or business retains payment-related data only*
- 15 *for a time period and in a manner explicitly permitted by the policy.*
- 16 (2) *Store sensitive authentication data subsequent to an*
- 17 *authorization, even if that data is encrypted. Sensitive*
- 18 *authentication data includes all of the following:*
- 19 (A) *The full contents of any data track from a payment card or*
- 20 *other payment device.*
- 21 (B) *The card verification code or any value used to verify*
- 22 *transactions when the payment device is not present.*
- 23 (C) *The personal identification number (PIN) or the encrypted*
- 24 *PIN block.*
- 25 (3) *Store any payment-related data that is not needed for*
- 26 *business, legal, or regulatory purposes.*
- 27 (4) *Store any of the following data elements:*
- 28 (A) *Payment verification code.*

1 (B) *Payment verification value.*

2 (C) *PIN verification value.*

3 (D) *Social security number.*

4 (E) *Driver's license number.*

5 (5) *Retain the primary account number unless retained in a*
6 *manner consistent with the other requirements of this subdivision*
7 *and in a form that is unreadable and unusable by unauthorized*
8 *persons anywhere it is stored.*

9 (6) *Send payment-related data over open, public networks unless*
10 *the data is encrypted using strong cryptography and security*
11 *protocols or otherwise rendered indecipherable.*

12 (7) *Fail to limit access to payment-related data to only those*
13 *individuals whose job requires that access.*

14 (b) (1) *This section shall not apply to any person or business*
15 *subject to Sections 6801 to 6809, inclusive, of Title 15 of the United*
16 *States Code and state or federal statutes or regulations*
17 *implementing those sections, if the person or business is subject*
18 *to compliance oversight by a state or federal regulatory agency*
19 *with respect to those sections.*

20 (2) *Nothing in this section shall prohibit a person or business*
21 *that sells goods or services to any California resident and accepts*
22 *as payment a credit card, debit card, or other payment device from*
23 *storing payment-related data for the sole purpose of processing*
24 *ongoing or recurring payments, provided that the payment-related*
25 *data is maintained in accordance with this section.*

26 (c) *For purposes of this section, "payment-related data" means*
27 *any computerized information described in subdivision (h) of*
28 *Section 1798.82, whether individually or in combination with any*
29 *other information described in that paragraph.*

30 SEC. 2. *Section 1724.6 is added to the Civil Code, to read:*

31 1724.6. (a) *A person or business subject to Section 1724.4*
32 *shall be liable for the reimbursement of all reasonable and actual*
33 *costs of providing notice pursuant to subdivision (a) of Section*
34 *1798.82 and for the reasonable and actual cost of card replacement*
35 *as a result of a breach described in that section, to the owner or*
36 *licensee of the information.*

37 (b) *The liability of a person or business subject to Section 1724.4*
38 *to reimburse the owner or licensee may be excused, in whole or*
39 *in part, if the person or business can demonstrate compliance with*

1 *all provisions of Section 1724.4 at the time of the breach of security*
2 *of the system.*

3 *SEC. 3. Section 1798.81.5 of the Civil Code is amended to*
4 *read:*

5 1798.81.5. (a) (1) It is the intent of the Legislature to ensure
6 that personal information about California residents is protected.
7 To that end, the purpose of this section is to encourage businesses
8 that ~~own or license~~ *own, license, or maintain* personal information
9 about Californians to provide reasonable security for that
10 information. ~~For~~

11 (2) ~~For the purpose of this section, the phrase “owns or licenses”~~
12 ~~is intended to include, but is not limited to, terms “own” and~~
13 ~~“license” include~~ personal information that a business retains as
14 part of the business’ internal customer account or for the purpose
15 of using that information in transactions with the person to whom
16 the information relates. *The term “maintain” includes personal*
17 *information that a business maintains but does not own or license.*

18 (b) A business that ~~owns or licenses~~ *owns, licenses, or maintains*
19 personal information about a California resident shall implement
20 and maintain reasonable security procedures and practices
21 appropriate to the nature of the information, to protect the personal
22 information from unauthorized access, destruction, use,
23 modification, or disclosure.

24 (c) A business that discloses personal information about a
25 California resident pursuant to a contract with a nonaffiliated third
26 party *that is not subject to subdivision (b)* shall require by contract
27 that the third party implement and maintain reasonable security
28 procedures and practices appropriate to the nature of the
29 information, to protect the personal information from unauthorized
30 access, destruction, use, modification, or disclosure.

31 (d) For purposes of this section, the following terms have the
32 following meanings:

33 (1) “Personal information” means an individual’s first name or
34 first initial and his or her last name in combination with any one
35 or more of the following data elements, when either the name or
36 the data elements are not encrypted or redacted:

37 (A) Social security number.

38 (B) Driver’s license number or California identification card
39 number.

1 (C) Account number, credit or debit card number, in
2 combination with any required security code, access code, or
3 password that would permit access to an individual’s financial
4 account.

5 (D) Medical information.

6 (2) “Medical information” means any individually identifiable
7 information, in electronic or physical form, regarding the
8 individual’s medical history or medical treatment or diagnosis by
9 a health care professional.

10 (3) “Personal information” does not include publicly available
11 information that is lawfully made available to the general public
12 from federal, state, or local government records.

13 (e) The provisions of this section do not apply to any of the
14 following:

15 (1) A provider of health care, health care service plan, or
16 contractor regulated by the Confidentiality of Medical Information
17 Act (Part 2.6 (commencing with Section 56) of Division 1).

18 (2) A financial institution as defined in Section 4052 of the
19 Financial Code and subject to the California Financial Information
20 Privacy Act (Division 1.2 (commencing with Section 4050) of the
21 Financial Code.

22 (3) A covered entity governed by the medical privacy and
23 security rules issued by the federal Department of Health and
24 Human Services, Parts 160 and 164 of Title 45 of the Code of
25 Federal Regulations, established pursuant to the Health Insurance
26 Portability and Availability Act of 1996 (HIPAA).

27 (4) An entity that obtains information under an agreement
28 pursuant to Article 3 (commencing with Section 1800) of Chapter
29 1 of Division 2 of the Vehicle Code and is subject to the
30 confidentiality requirements of the Vehicle Code.

31 (5) A business that is regulated by state or federal law providing
32 greater protection to personal information than that provided by
33 this section in regard to the subjects addressed by this section.
34 Compliance with that state or federal law shall be deemed
35 compliance with this section with regard to those subjects. This
36 paragraph does not relieve a business from a duty to comply with
37 any other requirements of other state and federal law regarding
38 the protection and privacy of personal information.

39 ~~SECTION 4.~~

40 *SEC. 4.* Section 1798.82 of the Civil Code is amended to read:

1 1798.82. (a) A person or business that conducts business in
2 California, and that owns or licenses computerized *or*
3 *noncomputerized* data that includes personal information, shall
4 disclose a breach of the security of the system following discovery
5 or notification of the breach in the security of the data to a resident
6 of California whose ~~unencrypted~~ personal information was, or is
7 reasonably believed to have been, acquired by an unauthorized
8 person. The disclosure shall be made in the most expedient time
9 possible and without unreasonable delay, consistent with the
10 legitimate needs of law enforcement, as provided in subdivision
11 (c), or any measures necessary to determine the scope of the breach
12 and restore the reasonable integrity of the data system.

13 (b) (1) A person or business that maintains computerized *or*
14 *noncomputerized* data that includes personal information that the
15 person or business does not own shall notify the owner or licensee
16 of the information of the breach of the security of the data
17 immediately following discovery, if the personal information was,
18 or is reasonably believed to have been, acquired by an unauthorized
19 person.

20 (2) *In addition to notifying the owner of the data, the person or*
21 *business that maintains the data shall notify persons affected by*
22 *the breach within 15 days of the breach using the following*
23 *methods:*

24 (A) *Email notice if the person or business has an email address*
25 *for the subject persons.*

26 (B) *Conspicuous posting of the notice on the Internet Web site*
27 *page of the person or business, if the person or business maintains*
28 *an Internet Web site page, for at least 30 days.*

29 (C) *Notification to major statewide media.*

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

35 (d) A person or business that is required to issue a security
36 breach notification pursuant to this section shall meet all of the
37 following requirements:

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

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

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

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

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

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

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

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

22 (G) *If the person or business providing the notification was the*
23 *source of the breach, an offer to provide appropriate identity theft*
24 *prevention and mitigation services, such as credit monitoring,*
25 *shall be provided at no cost to the affected person for not less than*
26 *24 months, along with all information necessary to take advantage*
27 *of the offer to any person whose information was or may have been*
28 *breached if the breach exposed or may have exposed personal*
29 *information defined in paragraph (1) of subdivision (h).*

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

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

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

36 (4) In the case of a breach of the security of the system involving
37 personal information defined in paragraph (2) of subdivision (h)
38 for an online account, and no other personal information defined
39 in paragraph (1) of subdivision (h), the person or business may
40 comply with this section by providing the security breach

1 notification in electronic or other form that directs the person whose
2 personal information has been breached promptly to change his
3 or her password and security question or answer, as applicable, or
4 to take other steps appropriate to protect the online account with
5 the person or business and all other online accounts for which the
6 person whose personal information has been breached uses the
7 same user name or email address and password or security question
8 or answer.

9 (5) In the case of a breach of the security of the system involving
10 personal information defined in paragraph (2) of subdivision (h)
11 for login credentials of an email account furnished by the person
12 or business, the person or business shall not comply with this
13 section by providing the security breach notification to that email
14 address, but may, instead, comply with this section by providing
15 notice by another method described in subdivision (j) or by clear
16 and conspicuous notice delivered to the resident online when the
17 resident is connected to the online account from an Internet
18 Protocol address or online location from which the person or
19 business knows the resident customarily accesses the account.

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

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

36 (g) For purposes of this section, “breach of the security of the
37 system” means unauthorized acquisition of computerized *or*
38 *noncomputerized* data that compromises the security,
39 confidentiality, or integrity of personal information maintained by
40 the person or business. Good faith acquisition of personal

1 information by an employee or agent of the person or business for
2 the purposes of the person or business is not a breach of the security
3 of the system, provided that the personal information is not used
4 or subject to further unauthorized disclosure.

5 (h) For purposes of this section, “personal information” means
6 either of the following:

7 (1) An individual’s first name or first initial and last name in
8 combination with any one or more of the following data elements,
9 ~~when either the name or the data elements are not encrypted:~~
10 *elements*:

11 (A) Social security number.

12 (B) Driver’s license number or California identification card
13 number.

14 (C) Account number, credit or debit card number, in
15 combination with any required security code, access code, or
16 password that would permit access to an individual’s financial
17 account.

18 (D) Medical information.

19 (E) Health insurance information.

20 (2) A user name or email address, in combination with a
21 password or security question and answer that would permit access
22 to an online account.

23 (i) (1) For purposes of this section, “personal information” does
24 not include publicly available information that is lawfully made
25 available to the general public from federal, state, or local
26 government records.

27 (2) For purposes of this section, “medical information” means
28 any information regarding an individual’s medical history, mental
29 or physical condition, or medical treatment or diagnosis by a health
30 care professional.

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

36 (j) For purposes of this section, “notice” may be provided by
37 one of the following methods:

38 (1) Written notice.

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

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

10 (A) Email notice when the person or business has an email
11 address for the subject persons.

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

15 (C) Notification to major statewide media.

16 (k) Notwithstanding subdivision (j), a person or business that
17 maintains its own notification procedures as part of an information
18 security policy for the treatment of personal information and is
19 otherwise consistent with the timing requirements of this part, shall
20 be deemed to be in compliance with the notification requirements
21 of this section if the person or business notifies subject persons in
22 accordance with its policies in the event of a breach of security of
23 the system.

24 *SEC. 5. Section 1798.84 of the Civil Code is amended to read:*

25 1798.84. (a) Any waiver of a provision of this title is contrary
26 to public policy and is void and unenforceable.

27 (b) *In addition to any other available remedies for a violation*
28 *of this title, a public prosecutor authorized pursuant to Section*
29 *17204 of the Business and Professions Code may bring an action*
30 *to recover a civil penalty not exceeding five hundred dollars (\$500)*
31 *per violation, or, in the case of a willful, intentional, or reckless*
32 *violation, a penalty not exceeding three thousand dollars (\$3,000)*
33 *per violation.*

34 ~~(b)~~

35 (c) Any customer injured by a violation of this title may institute
36 a civil action to recover damages.

37 ~~(e)~~

38 (d) In addition, for a willful, intentional, or reckless violation
39 of Section 1798.83, a customer may recover a civil penalty not to
40 exceed three thousand dollars (\$3,000) per violation; otherwise,

1 the customer may recover a civil penalty of up to five hundred
2 dollars (\$500) per violation for a violation of Section 1798.83.

3 ~~(d)~~

4 (e) Unless the violation is willful, intentional, or reckless, a
5 business that is alleged to have not provided all the information
6 required by subdivision (a) of Section 1798.83, to have provided
7 inaccurate information, failed to provide any of the information
8 required by subdivision (a) of Section 1798.83, or failed to provide
9 information in the time period required by subdivision (b) of
10 Section 1798.83, may assert as a complete defense in any action
11 in law or equity that it thereafter provided regarding the information
12 that was alleged to be untimely, all the information, or accurate
13 information, to all customers who were provided incomplete or
14 inaccurate information, respectively, within 90 days of the date
15 the business knew that it had failed to provide the information,
16 timely information, all the information, or the accurate information,
17 respectively.

18 ~~(e)~~

19 (f) Any business that violates, proposes to violate, or has violated
20 this title may be enjoined.

21 ~~(f)~~

22 (g) (1) A cause of action shall not lie against a business for
23 disposing of abandoned records containing personal information
24 by shredding, erasing, or otherwise modifying the personal
25 information in the records to make it unreadable or undecipherable
26 through any means.

27 (2) The Legislature finds and declares that when records
28 containing personal information are abandoned by a business, they
29 often end up in the possession of a storage company or commercial
30 landlord. It is the intent of the Legislature in paragraph (1) to create
31 a safe harbor for such a record custodian who properly disposes
32 of the records in accordance with paragraph (1).

33 ~~(g)~~

34 (h) A prevailing plaintiff in any action commenced under
35 Section 1798.83 shall also be entitled to recover his or her
36 reasonable attorney's fees and costs.

37 ~~(h)~~

38 (i) The rights and remedies available under this section are
39 cumulative to each other and to any other rights and remedies
40 available under law.

1 *SEC. 6. Section 1798.85 of the Civil Code is amended to read:*

2 1798.85. (a) Except as provided in this section, a person or
3 entity may not do any of the following:

4 (1) Publicly post or publicly display in any manner an
5 individual's social security number. "Publicly post" or "publicly
6 display" means to intentionally communicate or otherwise make
7 available to the general public.

8 (2) Print an individual's social security number on any card
9 required for the individual to access products or services provided
10 by the person or entity.

11 (3) Require an individual to transmit his or her social security
12 number over the Internet, unless the connection is secure or the
13 social security number is encrypted.

14 (4) Require an individual to use his or her social security number
15 to access an Internet Web site, unless a password or unique
16 personal identification number or other authentication device is
17 also required to access the Internet Web site.

18 (5) Print an individual's social security number on any materials
19 that are mailed to the individual, unless state or federal law requires
20 the social security number to be on the document to be mailed.
21 Notwithstanding this paragraph, social security numbers may be
22 included in applications and forms sent by mail, including
23 documents sent as part of an application or enrollment process, or
24 to establish, amend or terminate an account, contract or policy, or
25 to confirm the accuracy of the social security number. A social
26 security number that is permitted to be mailed under this section
27 may not be printed, in whole or in part, on a postcard or other
28 mailer not requiring an envelope, or visible on the envelope or
29 without the envelope having been opened.

30 (6) *Sell, advertise for sale, or offer to sell an individual's social*
31 *security number.*

32 (b) This section does not prevent the collection, use, or release
33 of a social security number as required by state or federal law or
34 the use of a social security number for internal verification or
35 administrative purposes.

36 (c) This section does not prevent an adult state correctional
37 facility, an adult city jail, or an adult county jail from releasing an
38 inmate's social security number, with the inmate's consent and
39 upon request by the county veterans service officer or the United
40 States Department of Veterans Affairs, for the purposes of

1 determining the inmate's status as a military veteran and his or her
2 eligibility for federal, state, or local veterans' benefits or services.

3 (d) This section does not apply to documents that are recorded
4 or required to be open to the public pursuant to Chapter 3.5
5 (commencing with Section 6250), Chapter 14 (commencing with
6 Section 7150) or Chapter 14.5 (commencing with Section 7220)
7 of Division 7 of Title 1 of, Article 9 (commencing with Section
8 11120) of Chapter 1 of Part 1 of Division 3 of Title 2 of, or Chapter
9 9 (commencing with Section 54950) of Part 1 of Division 2 of
10 Title 5 of, the Government Code. This section does not apply to
11 records that are required by statute, case law, or California Rule
12 of Court, to be made available to the public by entities provided
13 for in Article VI of the California Constitution.

14 (e) (1) In the case of a health care service plan, a provider of
15 health care, an insurer or a pharmacy benefits manager, a contractor
16 as defined in Section 56.05, or the provision by any person or
17 entity of administrative or other services relative to health care or
18 insurance products or services, including third-party administration
19 or administrative services only, this section shall become operative
20 in the following manner:

21 (A) On or before January 1, 2003, the entities listed in paragraph
22 (1) shall comply with paragraphs (1), (3), (4), and (5) of subdivision
23 (a) as these requirements pertain to individual policyholders or
24 individual contractholders.

25 (B) On or before January 1, 2004, the entities listed in paragraph
26 (1) shall comply with paragraphs (1) to (5), inclusive, of
27 subdivision (a) as these requirements pertain to new individual
28 policyholders or new individual contractholders and new groups,
29 including new groups administered or issued on or after January
30 1, 2004.

31 (C) On or before July 1, 2004, the entities listed in paragraph
32 (1) shall comply with paragraphs (1) to (5), inclusive, of
33 subdivision (a) for all individual policyholders and individual
34 contractholders, for all groups, and for all enrollees of the Healthy
35 Families and Medi-Cal programs, except that for individual
36 policyholders, individual contractholders and groups in existence
37 prior to January 1, 2004, the entities listed in paragraph (1) shall
38 comply upon the renewal date of the policy, contract, or group on
39 or after July 1, 2004, but no later than July 1, 2005.

1 (2) A health care service plan, a provider of health care, an
2 insurer or a pharmacy benefits manager, a contractor, or another
3 person or entity as described in paragraph (1) shall make reasonable
4 efforts to cooperate, through systems testing and other means, to
5 ensure that the requirements of this article are implemented on or
6 before the dates specified in this section.

7 (3) Notwithstanding paragraph (2), the Director of the
8 Department of Managed Health Care, pursuant to the authority
9 granted under Section 1346 of the Health and Safety Code, or the
10 Insurance Commissioner, pursuant to the authority granted under
11 Section 12921 of the Insurance Code, and upon a determination
12 of good cause, may grant extensions not to exceed six months for
13 compliance by health care service plans and insurers with the
14 requirements of this section when requested by the health care
15 service plan or insurer. Any extension granted shall apply to the
16 health care service plan or insurer's affected providers, pharmacy
17 benefits manager, and contractors.

18 (f) If a federal law takes effect requiring the United States
19 Department of Health and Human Services to establish a national
20 unique patient health identifier program, a provider of health care,
21 a health care service plan, a licensed health care professional, or
22 a contractor, as those terms are defined in Section 56.05, that
23 complies with the federal law shall be deemed in compliance with
24 this section.

25 (g) A person or entity may not encode or embed a social security
26 number in or on a card or document, including, but not limited to,
27 using a barcode, chip, magnetic strip, or other technology, in place
28 of removing the social security number, as required by this section.

29 (h) This section shall become operative, with respect to the
30 University of California, in the following manner:

31 (1) On or before January 1, 2004, the University of California
32 shall comply with paragraphs (1), (2), and (3) of subdivision (a).

33 (2) On or before January 1, 2005, the University of California
34 shall comply with paragraphs (4) and (5) of subdivision (a).

35 (i) This section shall become operative with respect to the
36 Franchise Tax Board on January 1, 2007.

37 (j) This section shall become operative with respect to the
38 California community college districts on January 1, 2007.

39 (k) This section shall become operative with respect to the
40 California State University system on July 1, 2005.

1 (l) This section shall become operative, with respect to the
2 California Student Aid Commission and its auxiliary organization,
3 in the following manner:

4 (1) On or before January 1, 2004, the commission and its
5 auxiliary organization shall comply with paragraphs (1), (2), and
6 (3) of subdivision (a).

7 (2) On or before January 1, 2005, the commission and its
8 auxiliary organization shall comply with paragraphs (4) and (5)
9 of subdivision (a).

10 (m) *In addition to any other available remedies for a violation*
11 *of this title, a public prosecutor authorized pursuant to Section*
12 *17204 of the Business and Professions Code may bring an action*
13 *to recover a civil penalty not exceeding five hundred dollars (\$500)*
14 *per violation.*