

ANALYSIS OF ORIGINAL BILL

Franchise Tax Board

Author: Ruskin Analyst: Deborah Barrett Bill Number: AB 703
Related Bills: See Legislative History Telephone: 845-4301 Introduced Date: February 22, 2007
Attorney: Tommy Leung Sponsor: _____

SUBJECT: Security of Social Security Numbers

SUMMARY

This bill would require that employees, customers, and customer accounts be identified by a number other than a social security number (SSN).

PURPOSE OF THE BILL

According to the author's staff, the purpose of this bill is to protect SSN information from identity theft.

EFFECTIVE/OPERATIVE DATE

This bill would be effective on January 1, 2008, and be operative on or after that date.

POSITION

Pending.

ANALYSIS

FEDERAL/STATE LAW

Current state law prohibits a person or entity from the following:

- Publicly posting or displaying in any manner an individual's SSN,
- Printing or embedding an individual's SSN on any card required for the individual to access products or services provided by the person or entity,
- Requiring an individual to transmit an SSN over the Internet, unless the connection is secure or the SSN is encrypted,
- Requiring the use of an SSN to access an Internet Web site, unless a password or personal identification number or authentication device is also required for access,

Board Position:

_____ S _____ NA _____ NP
_____ SA _____ O _____ NAR
_____ N _____ OUA X PENDING

Department Director

Date

Lynette Iwafuchi
for Selvi Stanislaus

5/8/07

- Printing SSNs on any materials that are mailed to the person, unless required by federal or state law or the materials are to confirm the accuracy of the SSN, and
- In the instances where the use of an SSN meets the exceptions contained in current law, an SSN cannot be printed on a postcard or other mailer that does not require an envelope or would make the SSN visible without the envelope being opened.

Current law allows the collection, use, and release of an SSN as required by federal law or the use of an SSN for internal verification, including SSNs on documents mailed to third parties such as garnishments and levies. Current law also permits the display of SSNs that are required by specific statute, case law, or California Rules of Court to be made available to the public.

Current state tax law provides for fines and imprisonment for the unlawful disclosure of tax returns and return information. Current federal tax law provides that the unlawful disclosure of tax returns and return information is punishable as a felony.

THIS BILL

This bill would do the following:

- Require a person or entity to use a number or other identifier to identify an employee, customer, or customer account, rather than by SSN, except when required by federal or state law;
- Require records containing SSNs to be discarded or destroyed in a manner that protects confidentiality, such as through the use of crosscut shredding; and
- Require stored records containing SSNs in an electronic format to be encrypted or maintained in locked cabinets or locked storage.

PROGRAM BACKGROUND

The department currently collects personal information, including SSNs, from various sources, including the taxpayer and agencies required to report financial information. This information is used for compliance development, audit, and collection purposes. The SSN is used as the primary matching identifier from most sources of information collected. As required by statute, all information received from the taxpayer is confidential and is shared with federal or state agencies only for statutorily specified purposes. Franchise Tax Board (FTB) has stringent departmental policies and procedures regarding privacy and disclosure.

FTB uses a multitude of computing platforms, software, and data bases to facilitate its tax return processing, auditing, and collection functions. FTB secures all confidential documents in its possession, both electronic and paper, with a security standard that meets or exceeds IRS specifications and utilizes best industry standards. The portable computing devices (laptops) used by department personnel are encrypted. FTB's practice is to encrypt data while transmitting; current systems and databases that reside internally behind firewalls and other security mechanisms are not encrypted.

IMPLEMENTATION CONSIDERATIONS

The department has identified the following implementation concerns. Department staff is available to work with the author's office to resolve these and other concerns that may be identified.

Because this bill would require SSNs to be replaced, each agency that shares data with FTB would be required to assign a "unique identifier" for each taxpayer. Such a change would likely delay the data match processes between FTB and other state agencies because the unique identifier assigned in one state agency system may not be consistent with the identifier assigned by another. A new common identifier would have to be developed and incorporated with multiple state agency systems and processes. It is unlikely that this could be accomplished by the enactment date of this bill because of the immense amount of coordination that would be required to establish a statewide common identifier. It is recommended that the author provide a sufficient period for state agencies to incorporate the changes that would be required by this bill.

FTB currently utilizes an SSN on wage garnishments, levies, and state tax liens because this is the only common identifier between FTB, employers, lenders, and financial institutions. Without an alternative common identifier, the provisions of this bill would negatively impact FTB's ability to collect taxes and adversely affect the state income tax revenues.

This bill would require stored electronic records to be encrypted and kept in locked cabinets or locked storage. Based on discussions with the author's staff, the intent was that electronic records be encrypted, while paper records are to be maintained in locked cabinets or storage. It is recommended that the language be amended to clarify the author's intent.

Although FTB encrypts data when transmitting, data maintained within FTB systems are not encrypted and the provision that electronic records in storage be encrypted would require replacement of most of the legacy systems in place at FTB. Current encryption technology requires the encryption to be incorporated in the system development phase and cannot be readily added to current legacy systems. Recognizing the intent to provide more security to data containing SSNs, the author may wish to consider other security standards for protection of sensitive data that achieve equivalent levels of security as obtained through encryption.

Civil Code section 1798.85 (b) expressly permits the use of SSNs for internal verification purposes. This bill would expressly permit the application of this section while attempting to limit the use of SSNs. The author may wish to amend the bill to provide clarity about which should be given priority.

LEGISLATIVE HISTORY

SB 222 (Runner, 2005/06) would have added sanctions to existing law to prohibit acts compromising an individual's SSN. This bill was referred to the Committee on Public Safety and never heard.

AB 1811 (Bogh, 2003/04) would have prohibited the public posting or displaying of any portion of an individual's SSN. This bill was held in the Judiciary Committee.

AB 763 (Liu, Stats. 2003, Ch. 532) provides that in those circumstances where an SSN was permitted to be mailed, the SSN can not be mailed on a postcard or other mailer or be made visible on the envelope without the envelope having been opened.

SB25 (Bowen, Stats. 2003, Ch. 907) extends requirements restricting use of SSNs to state and local agencies, subject to specified exceptions or delayed operative dates.

OTHER STATES' INFORMATION

The states surveyed include *Florida, Illinois, Massachusetts, Michigan, Minnesota, and New York*. These states were selected due to their similarities to California's economy, business entity types, and tax laws. Most states have privacy laws that are similar to California's privacy laws and the federal Privacy Act prohibiting various state and local agencies from disclosing personal identifying information, such as an SSN, in an unauthorized manner. Some states have additional laws relating to identity theft; however, they do not further restrict disclosure and use of personal identifying information by revenue collecting agencies.

FISCAL IMPACT

Although FTB uses an internal FTB account number for taxpayer accounts, the accounts are referenced by SSN to coordinate the matching of external sources of data with the FTB account. To the extent that changes to external data disrupt current processes, alternative work processes and system reprogramming may be needed to facilitate the change in the collection and use of other identifiers anticipated by this bill's provisions. Encryption of internal data would require replacement of several legacy systems that would be costly and require significant resources to develop, test, and implement.

Fiscal costs will be developed as this bill progresses through the legislative process.

ECONOMIC IMPACT

Revenue Discussion

This bill would not impact state tax liabilities, but could impact the amount of revenue collected each year. FTB uses data from a wide variety of sources to enforce tax law. This bill would render some of these sources unusable for tax enforcement purposes resulting in unknown revenue losses.

LEGISLATIVE STAFF CONTACT

Deborah Barrett
Franchise Tax Board
(916) 845-4301
deborah.barrett@ftb.ca.gov

Brian Putler
Franchise Tax Board
(916) 845-6333
brian.putler@ftb.ca.gov