Internal Audit Department

ORANGE COUNTY

SPECIAL REPORT ON VIRTUAL TIMESHEET INTERFACE (VTI): ACCESS TO EMPLOYEE SOCIAL SECURITY NUMBERS

As of August 1, 2007

AUDIT NO: 2763 (FORMERLY 2631-3)
REPORT DATE: NOVEMBER 14, 2007

Corporate Controls:
Centralized Core Business System Audit

Audit Director: Peter Hughes, Ph.D., CPA
Deputy Director: Eli Littner, CPA, CIA
Sr. Audit Manager: Michael Goodwin, CPA, CIA
Audit Manager: Winnie Keung, CPA, CIA

OCgov.com
ORANGE COUNTY
Our Community. Our Commitment.

Internal Audit Department

2005 Recipient of the Institute of Internal Auditor's Award for Recognition of Commitment to Professional Excellence, Quality & Outreach

Independence • Objectivity • Integrity

ORANGE COUNTY OCgov.com
Our Community. Our Commitment.

Internal Audit Department

Providing Facts and Perspectives Countywide

Dr. Peter Hughes	**Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE**
Office of The Director	Certified Compliance & Ethics Professional (CCEP)
	Certified Information Technology Professional (CITP)
	Certified Internal Auditor (CIA)
	Certified Fraud Examiner (CFE)
E-mail:	peter.hughes@iad.ocgov.com
Eli Littner	**CPA, CIA, CFE, CFS, CISA**
Deputy Director	Certified Fraud Specialist (CFS)
	Certified Information Systems Auditor (CISA)
Michael J. Goodwin	**CPA, CIA**
Senior Audit Manager	
Alan Marcum	**MBA, CPA, CIA, CFE**
Senior Audit Manager	
Autumn McKinney	**CPA, CIA, CISA, CGFM**
Senior Audit Manager	Certified Government Financial Manager (CGFM)

Hall of Finance & Records

12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

Phone: (714) 834-5475 Fax: (714) 834-2880

To access and view audit reports or obtain additional information about the OC Internal Audit Department, visit our website: www.ocgov.com/audit

Orange County's Internal Audit — Fraud Hot-Line — 24/7 Fraud Hotline

OC Fraud Hotline (714) 834-3608

Letter from Director Peter Hughes

Transmittal Letter

AUDIT NO. 2763 **November 14, 2007**

TO: David E. Sundstrom, Auditor-Controller

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: Special Report on Virtual Timesheet Interface (VTI): Access to Employee Social Security Numbers

As a result of our Internal Control Reviews of the County's bi-weekly payroll processes and our continuing assessment of the Virtual Timecard Interface (VTI) system, an issue came to our attention, which we consider a **Significant Issue,** concerning the ability of certain users to access to employee Social Security numbers and annual leave balances in the VTI system. Our special report on this issue is attached for your review.

Please note we have a structured and rigorous **Follow-Up Audit** process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). As a matter of policy, our **first Follow-Up Audit** will begin at six months from the official release of the report. A copy of all our Follow-Up Audit reports is provided to the BOS as well as to all those individuals indicated on our standard routing distribution list.

The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our **second Follow-Up Audit** will now begin at 12 months from the release of the original report, by which time **all** audit recommendations are expected to be addressed and implemented.

We have attached a **Follow-Up Audit Report Form**. Your department should complete this template as our audit recommendation is implemented. When we perform our first Follow-Up Audit approximately six months from the date of this report, we will need to obtain the completed document to facilitate our review.

At the request of the AOC, we are to bring to their attention any audit recommendations we find still not implemented or mitigated after the second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for discussion.

Each month I submit an **Audit Status Report** to the BOS where I detail any material and significant audit findings released in reports during the prior month and the implementation status of audit recommendations as disclosed by our Follow-Up Audits. Accordingly, the results of this audit will be included in a future status report to the BOS.

As always, the Internal Audit Department is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report or recommendation.

ATTACHMENTS

Other recipients of this report are listed on the Internal Auditor's Report on page 1.

Table of Contents

Special Report on Virtual Timesheet Interface (VTI):
Access to Employee Social Security Numbers
Audit No 2763

As of August 1, 2007

INTERNAL AUDITOR'S REPORT

AUDIT NO. 2763 **NOVEMBER 14, 2007**

TO: David E. Sundstrom, Auditor-Controller

SUBJECT: Special Report on Virtual Timesheet Interface (VTI): Access to Employee Social Security Numbers

Audit Highlight:
We found that VTI enabled certain users to obtain complete Social Security numbers and annual leave balances for employees within their respective department/ agency.

Scope of Review

In the course of our continuing assessment of the bi-weekly payroll process and the Virtual Timecard Interface (VTI) system, an issue was identified concerning access and confidentiality of employee Social Security numbers. This special report discusses only this issue, and we have issued separate audit reports for our payroll reviews. Our review was conducted in accordance with professional standards established by the Institute of Internal Auditors.

Results

Because of the privacy risk, sensitivity, and the potential of misuse of employee Social Security numbers, we consider the items contained in this report to be **Significant Issues**, and accordingly, did ***not*** provide the specifics in this report. We did, however, immediately meet with you and your Information Technology staff to work towards immediate resolution of the issue. We have also provided **four recommendations** for immediate evaluation and implementation. See Attachment A for description of Report Item Classifications.

Virtual Timecard Interface

Beginning approximately FY 2000-01, the County began implementing an automated timekeeping and reporting system known as Virtual Timesheet Interface (VTI). The software was developed by IntelliTime Systems Corporation and is supported by Auditor-Controller Information Technology. VTI was initially tested in a few select departments and eventually was implemented by nearly all County departments/agencies.

VTI has eight different user roles (e.g., employee, supervisor, payroll clerk, etc.). Each user role has different rights, with different levels of access. We noted that VTI currently enables users in the **supervisory and payroll clerk roles** (anyone with permission to review and approve timesheets) to obtain complete Social Security numbers and annual leave balances for all employees within their respective department/agency, including management and executive level. This can be accomplished by accessing employee information screens and performing queries that are available in these user roles.

This access appears to be limited to employees within the user's own department/agency. It should be noted that we are not aware of any breaches or misuses of this information, nor the extent of knowledge by VTI users in the County to access this information.

Protecting the Confidentiality of Social Security Numbers

The California Office of Privacy Protection in the Department of Consumer Affairs has the statutorily mandated purpose of protecting the privacy of individuals' personal information. The Office of Privacy Protection has published recommended practices for protecting the confidentiality of Social Security numbers (SSNs) because of the role they have come to play in the marketplace, in identity theft and other forms of fraud. We have included their report as an attachment to this letter.

The California Code sections governing access and confidentiality of SSNs include:

- **Civil Code Sections 1798.85 – 1798.86**. The California Office of Privacy Protection developed recommended practices that address, but are not limited to, the provisions of these Civil Code Sections. One of these recommended practices, or *Fair Information Practice Principles*, involves limiting access to records containing SSNs only to those who need them for performance of their duties.

  Labor Code Section 226 – requires employers to use only the last four digits of SSNs if they are shown on payroll related documents. Employers must comply with this code by January 1, 2008.

Please refer to Attachment C - *Recommended Practices on Protecting the Confidentiality of Social Security Numbers* for further discussion of the above code sections.

Employee Identification Numbers

We note that VTI also uses employee ID numbers as system identifiers in addition to using SSNs. An analysis should be conducted to determine if SSNs are needed as identifiers in addition to employee ID numbers.

Because VTI is used nearly Countywide (exceptions are the Sheriff-Coroner and sections of the Probation Department), and SSNs are the most prevalent form of personal information that play a significant role in the recent growth of identity theft and other consumer fraud, we have developed the following recommendations, all which we consider to be Significant Issues, for immediate corrective action to minimize risk and exposure of this information.

We have also included a recommendation to evaluate the need to access employee annual leave balances, which is displayed with the SSNs; however, we acknowledge that employee leave information is personal and poses little risk for misuse.

Recommendation No. 1
We recommend that Auditor-Controller/Information Technology investigate the full extent and impact of the ability to access employee Social Security numbers and annual leave balances. The investigation should include whether this information can be accessed by other user roles assigned in the VTI system.

Auditor-Controller Management Response:
Concur: Based on the Internal Audit Department's findings, we conducted an investigation to further assess situations where Social Security numbers might be accessible in VTI, including annual leave balances search processes. A number of vulnerabilities were identified. We also identified an issue where supervisors could access employees who reported to other managers within their own agency. Corrective actions were taken on August 3, 2007 (noted below).

Additionally, an expanded review is currently underway and we will keep you posted on its progress.

Recommendation No. 2
We recommend that Auditor-Controller/Information Technology implement corrective action that restricts access to employee Social Security numbers in accordance with governing rules and regulations.

Auditor-Controller Management Response:
Concur: Corrective actions were taken based on our investigation, as discussed in the response to Recommendation No. 1. Specifically, the following actions were implemented:

- Masked the SSN field on the "User Opening Balance" screen for all roles;
- Masked the SSN field on the "User Maintenance" screen for all roles;
- Removed the SSN field on the "User Role/Range Assignment" screen for all roles;
- Removed the search capability from the "User Opening Balance" screen; and
- Eliminated time keepers' ability to search for employees not in the range assigned to them.

Recommendation No. 3
We recommend the Auditor-Controller evaluate whether Social Security numbers are necessary as identifiers when employee ID numbers are also utilized in VTI.

Auditor-Controller Management Response:
Concur: We have been aware of this issue and have been exploring options for the elimination of the Social Security number field in VTI. However, this field is still required because it is the primary key with which the CGI/AMS (AHRS) functions and interfaces with VTI. The cost to modify the existing process would be significant. Based on this, we are continuing efforts to further assess VTI to ensure access to Social Security numbers is properly restricted. Additionally, as the County of Orange moves forward in its assessment of a replacement for the current AHRS application, alternatives for eliminating the use of Social Security numbers as the primary key will be aggressively pursued. Finally, the removal of Social Security numbers as the primary key in the CAPS system has been identified as a strategic priority.

Recommendation No. 4
We recommend that if any breach or misuse of employee Social Security numbers is identified during the course of this investigation, that the Auditor-Controller explores the necessary measures for remediation, such as notification to employees and resulting actions to enable credit monitoring for unauthorized uses.

Auditor-Controller Management Response:
Concur: Our investigation did not identify any misuse of Social Security numbers. However, a number of vulnerabilities were identified and corrected, as noted in our response to Recommendation No. 2.

Acknowledgment

We appreciate the courtesy and cooperation extended to us by the personnel of the Auditor-Controller. If we can be of further assistance, please contact me or Eli Littner, Deputy Director, at (714) 834-5899 or Michael Goodwin, Senior Audit Manager, at (714) 834-6066.

Respectfully Submitted,

Peter Hughes, Ph.D., CPA
Director, Internal Audit Department

ATTACHMENTS

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Shaun Skelly, Senior Director, A-C Accounting and Technology
Phillip Daigneau, Assistant Auditor-Controller, A-C Information Technology
Toni Smart, Manager, A-C Internal Audit and Staff Services
Foreperson, Grand Jury
Darlene J. Bloom, Clerk of the Board of Supervisors

ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we will classify audit report items into three distinct categories:

- **Material Weaknesses:**
  Audit findings or a combination of Significant Issues that can result in financial liability and exposure to a department/agency and to the County as a whole. Management is expected to address "Material Weaknesses" brought to their attention immediately.

- **Significant Issues:**
  Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of processes or internal controls. Significant Issues do not present a material exposure throughout the County. They generally will require prompt corrective actions.

- **Control Findings and/or Efficiency/Effectiveness Issues:**
  Audit findings that require management's corrective action to implement or enhance processes and internal controls. Control Findings and Efficiency/Effectiveness issues are expected to be addressed within our follow-up process of six months, but no later than twelve months.

ATTACHMENT B: Auditor-Controller Management Responses

AUDITOR-CONTROLLER
COUNTY OF ORANGE

HALL OF FINANCE AND RECORDS
12 CIVIC CENTER PLAZA, ROOM 200
POST OFFICE BOX 567
SANTA ANA, CALIFORNIA 92702-0567

(714) 834-2450 FAX: (714) 834-2569

www.ac.ocgov.com

SHAUN M. SKELLY
SENIOR DIRECTOR
ACCOUNTING & TECHNOLOGY

JAN E. GRIMES
DIRECTOR
CENTRAL ACCOUNTING OPERATIONS

WILLIAM A. CASTRO
DIRECTOR
SATELLITE ACCOUNTING OPERATIONS

PHILLIP T. DAIGNEAU
DIRECTOR
INFORMATION TECHNOLOGY

DAVID E. SUNDSTROM, CPA
AUDITOR-CONTROLLER

RECEIVED
2007 OCT -1 AM 9:24
INTERNAL AUDIT DEPARTMENT

September 27, 2007

TO: Peter Hughes, Director, Internal Audit Department

SUBJECT: Confidential Draft Report: Audit Number 2631-3

Following is our response to the recommendations contained in your confidential draft report: Special Report on Virtual Timesheet Interface (VTI), Access to Employee Social Security Numbers.

Recommendation No. 1
We recommend that Auditor-Controller Information Technology investigate the full extent and impact of the ability to access employee Social Security numbers and annual leave balances. The investigation should include whether this information can be accessed by other user roles assigned in the VTI system.

Auditor-Controller Response
Concur: Based on the Internal Audit Department's findings, we conducted an investigation to further assess situations where Social Security numbers might be accessible in VTI, including annual leave balances search processes. A number of vulnerabilities were identified. We also identified an issue where supervisors could access employees who reported to other managers within their own agency. Corrective actions were taken on August 3, 2007 (noted below).

Additionally, an expanded review is currently underway and we will keep you posted on its progress.

Recommendation No. 2
We recommend that Auditor-Controller Information Technology implement corrective action that restricts access to employee Social Security numbers in accordance with governing rules and regulations:

Auditor-Controller Response
Concur: Corrective actions were taken based on our investigation, as discussed in the response to Recommendation No. 1. Specifically, the following actions were implemented:

- Masked the SSN field on the "User Opening Balance" screen for all roles;
- Masked the SSN field on the "User Maintenance" screen for all roles;
- Removed the SSN field on the "User Role/Range Assignment" screen for all roles;

ATTACHMENT B: Auditor-Controller Management Responses (continued)

- Removed the search capability from the "User Opening Balance" screen; and
- Eliminated time keepers' ability to search for employees not in the range assigned to them.

Recommendation No. 3
We recommend the Auditor-Controller evaluate whether Social Security numbers are necessary as identifiers when employee ID numbers are also utilized in VTI.

Auditor-Controller Response
Concur: We have been aware of this issue and have been exploring options for the elimination of the Social Security number field in VTI. However, this field is still required because it is the primary key with which the CGI/AMS (AHRS) functions and interfaces with VTI. The cost to modify the existing process would be significant. Based on this, we are continuing efforts to further assess VTI to ensure access to Social Security number is properly restricted. Additionally, as the County of Orange moves forward in its assessment of a replacement for the current AHRS application, alternatives for eliminating the use of Social Security numbers as the primary key will be aggressively pursued. Finally, the removal of Social Security numbers as the primary key in the CAPS system has been identified as a strategic priority.

Recommendation No. 4
We recommend that if any breach or misuse of employee Social Security numbers is identified during the course of this investigation, that the Auditor-Controller explores the necessary measures for remediation, such as notification to employees and resulting actions to enable credit monitoring for unauthorized uses.

Auditor-Controller Response
Concur: Our investigation did not identify any misuse of Social Security numbers. However, a number of vulnerabilities were identified and corrected, as noted in our response to Recommendation No. 2.

Thank you for the opportunity to respond to the confidential draft report. Please contact Phillip Daigneau at 834-6277 if you have any questions on our response.

David E. Sundstrom
Auditor-Controller

PTD:lr (Confidential Draft Audit-VTI/wg/lr)

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

OFFICE OF
Privacy
Protection

Recommended Practices on Protecting the Confidentiality of Social Security Numbers

April 2007

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

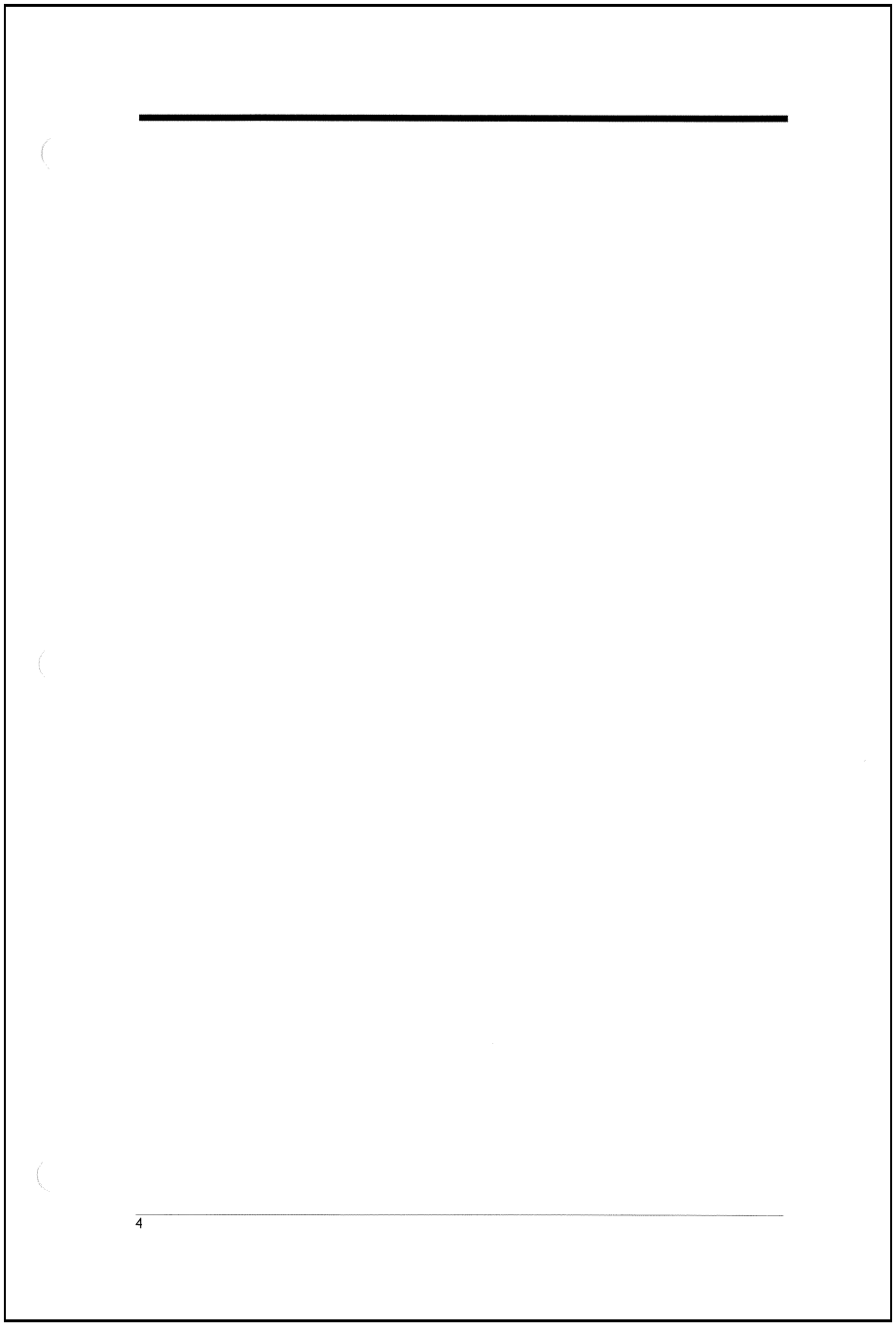
June 2002
Rev. January 2003
Rev. April 2007

California Office of Privacy Protection
www.privacy.ca.gov
866-785-9663

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Contents

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)



ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Introduction

The California Office of Privacy Protection in the Department of Consumer Affairs has the statutorily mandated purpose of "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices."[1] The law specifically directs the Office to "make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[2]

In fulfillment of those obligations, the Office of Privacy Protection is publishing these recommended practices for protecting the confidentiality of Social Security numbers. While many of the recommendations might be applied to protect any sensitive personal information, the focus is on Social Security numbers because of the role they have come to play in the marketplace and in identity theft and other forms of fraud.

In developing the recommendations, the Office of Privacy Protection received consultation and advice from an advisory committee made up of representatives of the financial, insurance, health care, retail and information industries and of consumer privacy advocates.[3] The committee members' contributions were very helpful and are greatly appreciated.

Unique Status of SSN As a Privacy Risk

The Social Security number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential.[4]

Created by the federal government in 1936 to track workers' earnings and eligibility for retirement benefits, the SSN is now used in both the public and private sectors for a myriad of purposes totally unrelated to this original purpose. It is used so widely because the SSN is a unique identifier that does not change, allowing it to serve many record management purposes.[5]

Today SSNs are used as representations of individual identity, as secure passwords, and as the keys for linking multiple records together. The problem is that these uses are incompatible. The widespread use of the SSN as an individual identifier, resulting in its appearance on mailing labels, ID cards and badges, and various publicly displayed documents, makes it unfit to be a secure password providing access to financial records and other personal information.[6]

The broad use and public exposure of SSNs has been a major contributor to the tremendous growth in recent years in identity theft and other forms of credit fraud. The need to significantly reduce the risks to individuals of the inappropriate disclosure and misuse of SSNs, has in recent years led California and a few other states to take steps to limit their use and display.[7]

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

California Laws on SSN Confidentiality

Summary of Civil Code Sections 1798.85-1798.86

Civil Code Sections 1798.85-1798.86 took effect beginning July 1, 2002 and was phased in through January 1, 2007. It applies to any person or entity and prohibits the following practices:

- Posting or publicly display SSNs,
- Printing SSNs on identification cards or badges,
- Requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted,
- Requiring people to log onto a web site using an SSN without a password, and
- Printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.[9]

Text of Civil Code Sections 1798.85-1798.86

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

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

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

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

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

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

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

(c) This section does not apply to documents that are recorded or required to be open to the public pursuant to Chapter 3.5 (commencing with Section 6250), Chapter 14 (commencing with Section 7150) or Chapter 14.5 (commencing with Section 7220) of Division 7 of Title 1 of, Article 9 (commencing with Section 11120) of Chapter 1 of Part 1 of Division 3 of Title 2 of, or Chapter 9 (commencing with Section 54950) of Part 1 of Division 2 of Title 5 of, the Government Code. This section does not apply to records that are required by statute, case law, or California Rule of Court, to be made

6

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

available to the public by entities provided for in Article VI of the California Constitution.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(k) This section shall become operative, with respect to the California Student Aid Commission and its auxiliary organization, in the follow-

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

ing manner:

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

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

1798.86. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

Summary of Labor Code Section 226

Labor Code Section 226 requires employers to print no more than the last four digits of an employee's SSN, or to use an employee ID number other than the SSN, on employee pay stubs or itemized statements. Employers must comply by January 1, 2008.

Text of Labor Code Section 226

226. (a) Every employer shall, semimonthly or at the time of each payment of wages, furnish each of his or her employees, either as a detachable part of the check, draft, or voucher paying the employee's wages, or separately when wages are paid by personal check or cash, an accurate itemized statement in writing showing

(1) gross wages earned,

(2) total hours worked by the employee, except for any employee whose compensation is solely based on a salary and who is exempt from payment of overtime under subdivision (a) of Section 515 or any applicable order of the Industrial Welfare Commission,

(3) the number of piece-rate units earned and any applicable piece rate if the employee is paid on a piece-rate basis,

(4) all deductions, provided that all deductions made on written orders of the employee may be aggregated and shown as one item,

(5) net wages earned,

(6) the inclusive dates of the period for which the employee is paid,

(7) the name of the employee and his or her social security number, except that by January 1, 2008, only the last four digits of his or her social security number or an employee identification number other than a social security number may be shown on the itemized statement,

(8) the name and address of the legal entity that is the employer, and

(9) all applicable hourly rates in effect during the pay period and the corresponding number of hours worked at each hourly rate by the employee. The deductions made from payments of wages shall be recorded in ink or other indelible form, properly dated, showing the month, day, and year, and a copy of the statement or a record of the deductions shall be kept on file by the employer for at least three years at the place of employment or at a central location within the State of California.

(b) An employer that is required by this code or any regulation adopted pursuant to this code to keep the information required by subdivision (a) shall afford current and former employees the right to inspect or copy the records pertaining to that current or former employee, upon reasonable request to the employer. The employer may take reasonable steps to assure the identity of a current or former employee. If the employer provides copies of the records, the actual cost of reproduction may be charged to the current or former employee.

(c) An employer who receives a written or oral request to inspect or copy records pursuant to subdivision (b) pertaining to a current or former employee shall comply with the request as soon as practicable, but no later than 21 calendar days from the date of the request. A violation of this subdivision is an infraction. Impossibility of performance, not caused by or a result of a violation of law, shall be an affirmative defense for an employer in any action alleging a violation of this subdivision. An employer may designate the person to whom a request under this subdivision will be made.

(d) This section does not apply to any employer of any person employed by the owner or occupant of a residential dwelling whose duties are incidental to the ownership, maintenance, or use of the dwelling, including the care and su-

8

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

pervision of children, or whose duties are personal and not in the course of the trade, business, profession, or occupation of the owner or occupant.

(e) An employee suffering injury as a result of a knowing and intentional failure by an employer to comply with subdivision (a) is entitled to recover the greater of all actual damages or fifty dollars ($50) for the initial pay period in which a violation occurs and one hundred dollars ($100) per employee for each violation in a subsequent pay period, not exceeding an aggregate penalty of four thousand dollars ($4,000), and is entitled to an award of costs and reasonable attorney's fees.

(f) A failure by an employer to permit a current or former employee to inspect or copy records within the time set forth in subdivision (c) entitles the current or former employee or the Labor Commissioner to recover a seven-hundred-fifty-dollar ($750) penalty from the employer.

(g) An employee may also bring an action for injunctive relief to ensure compliance with this section, and is entitled to an award of costs and reasonable attorney's fees.

(h) This section does not apply to the state, to any city, county, city and county, district, or to any other governmental entity, except that if the state or a city, county, city and county, district, or other governmental entity furnishes its employees with a check, draft, or voucher paying the employee's wages, the state or a city, county, city and county, district, or other governmental entity shall, by January 1, 2008, use no more than the last four digits of the employee's social security number or shall use an employee identification number other than the social security number on the itemized statement provided with the check, draft, or voucher.

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Recommended Practices

Fair Information Practice Principles

In developing these recommendations, the California Office of Privacy Protection looked first to the widely accepted principles that form the basis of most privacy laws in the United States, Canada, Europe, and other parts of the world. The Fair Information Practice Principles are openness, collection limitation, purpose specification, use limitation, data quality, individual participation, security and accountability.[12] While they were developed to guide the drafting of national privacy legislation, the principles are also appropriate for organizations to follow in developing their privacy policies and practices. The practices recommended here all derived from these basic privacy principles.

The Office of Privacy Protection's recommendations are intended to serve as guidelines to assist organizations in moving towards the goal of aligning their practices with the widely accepted fair information practice principles described below. These recommended practices address, but are not limited to, the provisions of California Civil Code section 1798.85.

The recommendations are relevant for private and public sector organizations, and they apply to the handling of all Social Security numbers in the possession of an organization: those of customers, employees, and business partners.

Reduce the collection of SSNs.
Fair Information Practice Principles: Collection Limitation, Use Limitation

- Collect SSNs preferably only where required to do so by federal or state law.
- When collecting SSNs as allowed, but not required, by law, do so only as reasonably necessary for the proper administration of lawful business activities.
- If a unique personal identifier is needed, develop your own as a substitute for the SSN.

Inform individuals when you request their SSNs.
Fair Information Practice Principle: Openness, Purpose Specification

- Whenever you collect SSNs as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, whether the law requires the number to be provided or not, and the consequences of not providing the number.
- If required by law, notify individuals (customers, employees, business partners, etc) annually of their right to request that you do not post or publicly display their SSN or do any of the other things prohibited in Civil Code Section 1798.85(a).

Eliminate the public display of SSNs.
Fair Information Practice Principle: Security

- Do not put SSNs on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, bulletin board postings, and other materials.
- Do not send documents with SSNs on them through the mail, except on applications or forms or when required by law.[13]

10

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

- When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.
- Do not send SSNs by email unless the connection is secure or the SSN is encrypted.
- Do not require an individual to send his or her SSN over the Internet or by email, unless the connection is secure or the SSN is encrypted.
- Do not require individuals to use SSNs as passwords or codes for access to Internet web sites or other services.

Control access to SSNs.
Fair Information Practice Principle: Security

- Limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.
- Use logs or electronic audit trails to monitor employees' access to records with SSNs.
- Protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
- Do not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
- Avoid sharing SSNs with other companies or organizations except where required by law.
- If you do share SSNs with other companies or organizations, including contractors, use written agreements to protect their confidentiality.
- Prohibit such third parties from re-disclosing SSNs, except as required by law.
- Require such third parties to use effective security controls on record systems containing SSNs.
- Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.
- If SSNs are disclosed inappropriately and the individuals whose SSNs were disclosed are put at risk of identity theft or other harm, promptly notify the individuals potentially affected.

Protect SSNs with security safeguards.
Fair Information Practice Principle: Security

- Develop a written security plan for record systems that contain SSNs.
- Develop written policies for protecting the confidentiality of SSNs, including but not limited to the following:
- Adopt "clean desk/work area" policy requiring employees to properly secure records containing SSNs.
- Do not leave voice mail messages containing SSNs and if you must send an SSN by fax, take special measures to ensure confidentiality.
- Require employees to ask individuals (employees, customers, etc.) for identifiers other than the SSN when looking up records for the individual.
- Require employees to promptly report any inappropriate disclosure or loss of records containing SSNs to their supervisors or to the organization's privacy officer.

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

- When discarding or destroying records in any medium containing SSNs, do so in a way that protects their confidentiality, such as shredding.[14]

Make your organization accountable for protecting SSNs.

Fair Information Practice Principle: Accountability

- Provide training and written material for employees on their responsibilities in handling SSNs.
- Conduct training at least annually.
- Train all new employees, temporary employees and contract employees.
- Impose discipline on employees for non-compliance with organizational policies and practices for protecting SSNs.
- Conduct risk assessments and regular audits of record systems containing SSNs.
- Designate someone in the organization as responsible for ensuring compliance with policies and procedures for protecting SSNs.

12

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Notes

[1] California Business & Professions Code section 350, subdivision (a).

[2] California Business & Professions Code section 350, subdivision(c).

[3] The Advisory Committee members were Victoria Allen of the California Credit Union League; Jennie Bretschneider, Legislative Aide to Senator Debra Bowen; James W. Bruner, Jr., of Orrick, Herrington & Sutcliffe; Shelley Curran of Consumers Union; Mari Frank, Esq., privacy consultant; Beth Givens of the Privacy Rights Clearinghouse; Tony Hadley of Experian; Michael Hensley of LexisNexis; Chris Lewis of Providian and the California Chamber of Commerce; Deborah Pierce of Privacy Activism; Rebecca Richards of TRUSTe; Wendy Schmidt of Federated Department Stores and the California Retailers Association; Elaine Torres of Wells Fargo Bank; and Lee Wood of the Association of California Life & Health Insurance Companies.

[4] Mark Rotenberg, Executive Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, "Testimony and Statement for the Record," Joint Hearing on SSNs and Identity Theft, Subcommittee on Oversight and Investigations, Committee on Financial Services, and Subcommittee on Social Security, Committee on Ways and Means, U. S. House of Representatives, November 8, 2001. Available at <www.epic.org/privacy/ssn/testimony_11_08_2001.html.>

[5] *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352, May 2002. Available at <www.gao.gov>.

[6] Chris Hibbert, Computer Professionals for Social Responsibility, *Frequently Asked Questions on SSNs and Privacy*, last modified February 16, 2002. Available at <www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html>.

[7] Arizona and Rhode Island prohibit the display of students' SSNs on the Internet. In Washington, as the result of an April 2000 executive order of the Governor, state agencies have removed SSNs from many documents where their display was determined not to be necessary. Minnesota's Government Data Practices Act classes SSNs as not public information.

[8] The Fair Information Practice Principles were first formulated by the U.S. Department of Health Education, and Welfare in 1973. They may be found in the Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at <www1.oecd.org/publications/e-book/930201E.PDF>. The principles are the following:

Openness: There should be a general policy of openness about the practices and policies with respect to personal information.

Collection Limitation: Personal information should be collected by lawful and fair means and with the knowledge or consent of the subject. Only the information necessary for the stated

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

purpose should be collected.

Purpose Specification: The purpose for collecting personal information should be specified at the time of collection. Further uses should be limited to those purposes.

Use Limitation: Personal information should not be used for purposes other than those specified, except with the consent of the subject or by the authority of law.

Data Quality: Personal information should be accurate, complete, timely and relevant to the purpose for which it is to be used.

Individual Participation: Individuals should have the right to inspect and correct their personal information.

Security: Personal information should be protected by reasonable security safeguards against such risks as unauthorized access, destruction, use, modification, and disclosure.

Accountability: Someone in an organization should be held accountable for compliance with the organization's privacy policy. Regular privacy audits and employee training should be conducted.

[9] See Appendix 1 for a partial list of federal laws and Appendix 2 for a partial list of federal and California laws that restrict the disclosure of SSNs.

[10] California Civil Code section 1798.81requires businesses to destroy customer records containing personal information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable, before discarding them.

14

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Appendix 1: Federal Laws Authorizing or Mandating SSNs

The following list of federal laws authorizing or mandating the collection and use of Social Security numbers is not comprehensive. It is taken from a report of the U.S. Government Accountability Office, *SSNs Are Widely Used by Government and Could Be Better Protected* (GAO-02-69IT of April , 2002).

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Tax Reform Act of 197642 U.S.C. 405(c)(2)(c)(i)	General public assistance programs, tax administration, driver's license, motorvehicle registration	Authorizes states to collect and use SSNs in administering any tax, general public assistance, driver's license, or motor vehicle registration law
Food Stamp Act of 19777 U.S.C. 2025(e)(1)	Food Stamp Program	Mandates the secretary of agriculture and state agencies to require SSNs for program participation
Deficit Reduction Act of 198442 U.S.C. 1320b-7(1)	Eligibility benefits under the Medicaid program	Requires that, as a condition of eligibility for Medicaid benefits, applicants for and recipients of these benefits furnish their SSNs to the state administering program
Housing and Community Development Act of 198742 U.S.C. 3543(a)	Eligibility for HUD programs	Authorizes the secretary of the Department of Housing and Urban Development to require applicants and participants in HUD programs to submit their SSNs as a condition of eligibility

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Federal Statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Family Support Act of 1988 42 U.S.C. 405(c)(2)(C)(ii)	Issuance of birth certificates	Requires states to obtain parents' SSNs before issuing a birth certificate unless there is good caue for not requiring the number
Technical and Miscellaneous Revenue Act of 1988 42 U.S.C. 405(c)(2)(D)(i)	Blood donation	Authorizes states and political subdivisions to require that blood donors provide their SSNs
Food, Agriculture, Conservation, and Trade Act of 1990 42 U.S.C. 405(c)(2)(C)	Retail and wholesale businesses participation in food stamp program	Authorizes the secretary of agriculture to require the SSNs of officers or owners of retail and wholesale food concerns that accept and redeem food stamps
Omnibus Budget Reconciliation Act of 1990 38 U.S.C. 510(c)	Eligibility for Veterans Affairs compensation or pension benefitsprograms	Requires individuals to provide their SSNs to be eligible for Department of Veterans Affairs' compensation or pension benefits programs
Social Security Independence and Program Improvements Act of 1994 42 U.S.C. 405(c)(2)(E)	Eligibility of potential jurors	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors
Personal Responsibility and WorkOpportunity Reconciliation Act of 1996 42 U.S.C. 666(a)(13)	Various license applications; divorce and child support documents; death certificates	Mandates that states have laws in effect that require collection of SSNs on applications for driver's licenses and other licenses; requires placement in the pertinent records of the SSN of the person subject to a divorce decree, child support order, paternity determination; requires SSNs on death certificates; creates national database for child support enforcement purposes

16

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Federal statute	General purpose for collecting or using SSN	Gpvernmemt entity and authorized or required use
Debt Collection Improvement Act of 1996 31 U.S.C. 7701(c)	Persons doing business with a federal agency	Requires those doing business with a federal agency, i.e., lenders in a federal guaranteed loan program; applicants for federal licenses, permits, right-of-ways, grants, or benefit payments; contractors of an agency and others to furnish SSNs to the agency
Higher Education Act Amendments of 1998 20 U.S.C. 1090(a)(7)	Financial assistance	Authorizes the secretary of education to include the SSNs of parents of dependent students on certain financial assistance forms
Internal Revenue Code(various amendments) 26 U.S.C. 6109	Tax returns	Authorizes the commissioner of the Internal Revenue Service to require that taxpayers include their SSNs on tax returns

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

Appendix 2: Federal and California Laws Restricting Disclosure of SSNs

Federal Laws

The following list of federal laws that restrict the disclosure of Social Security numbers is not comprehensive. It is taken from a U.S. Government Accountability Office report, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* (GAO-02-352, May 2002).

The Freedom of Information Act (5 U.S.C. 552)

This act establishes a presumption that records in the possession of agencies and departments of the executive branch of the federal government are accessible to the people. FOIA, as amended, provides that the public has a right of access to federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the federal government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold SSNs under this FOIA exemption. This statute does not apply to state and local governments.

The Privacy Act of 1974 (5 U.S.C. 552a)

The act regulates federal government agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records.[1] The act prohibits the disclosure of any record contained in a system of records unless the disclosure is made on the basis of a written request or prior written consent of the person to whom the records pertains, or is otherwise authorized by law. The act authorizes 12 exceptions under which an agency may disclose information in its records. However, these provisions do not apply to state and local governments, and state law varies widely regarding disclosure of personal information in state government agencies' control. There is one section of the Privacy Act, section 7, that does apply to state and local governments. Section 7 makes it unlawful for federal, state, and local agencies to deny an individual a right or benefit provided by law because of the individual's refusal to disclose his SSN. This provision does not apply (1) where federal law mandates disclosure of individuals' SSNs or (2) where a law existed prior to January 1, 1975 requiring disclosure of SSNs, for purposes of verifying the identity of individuals, to federal, state or local agencies maintaining a system of records existing and operating before that date. Section 7 also requires federal, state and local agencies, when requesting SSNs, to inform the individual (1) whether disclosure is voluntary or mandatory, (2) by what legal authority the SSN is solicited, and (3) what uses will be made of the SSN. The act contains a number of additional provisions that restrict federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or executive order of the president, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under federal programs.

The Social Security Act Amendments of 1990 (42 U.S.C. 405(c)(2)(C)(viii))

A provision of the Social Security Act bars disclosure by federal, state and local governments

18

ATTACHMENT C: Recommended Practices on Protecting the Confidentiality of Social Security Numbers (continued)

of SSNs collected pursuant to laws enacted on or after October 1, 1990. This provision of the act also contains criminal penalties for "unauthorized willful disclosures" of SSNs; the Department of Justice would determine whether to prosecute a willful disclosure violation. Because the act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by government entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore, would not restrict disclosing the SSN. Finally, because the provision applies to disclosure of SSNs collected pursuant to laws requiring SSNs, it is not clear if the provision also applies to disclosure of SSNs collected without a statutory requirement to do so. This provision applies to federal, state and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

California Laws

The following list of California laws restricting the disclosure of Social Security numbers is not comprehensive.

Confidentiality of Social Security Numbers (California Civil Code sections 1798.85 and 1786.60)

This law, bars businesses in California from publicly displaying SSNs in specified ways. It took effect beginning in July 2001 and ending with its full application to health care entities by January 2005. The law was intended to help control many of the common uses of SSNs that can expose people to the risk of identity theft.

Social Security Number Truncation on Pay Stubs (California Labor Code section 226)

This law requires employers to print no more than the last four digits of an employee's SSN, or to use an employee ID number other than the SSN, on employee pay stubs or itemized statements. Employers must comply by January 1, 2008.

Social Security Number Confidentiality in Family Court Records (California Family Code section 2024.5)

This law establishes a procedure for keeping SSNs confidential in court filings for legal separation, dissolution, or nullification of marriage.