
**OFFICE OF
THE INSPECTOR GENERAL**

SOCIAL SECURITY ADMINISTRATION

**UNIVERSITIES' USE OF SOCIAL
SECURITY NUMBERS AS STUDENT
IDENTIFIERS IN REGION IX**

November 2005

A-09-05-15099

AUDIT REPORT



Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the Congress, and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- Promote economy, effectiveness, and efficiency within the agency.**
- Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- Independence to determine what reviews to perform.**
- Access to all information necessary for the reviews.**
- Authority to publish findings and recommendations based on the reviews.**

Vision

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.



SOCIAL SECURITY

MEMORANDUM

Date: November 30, 2005

Refer To:

To: Peter D. Spencer
Regional Commissioner
San Francisco

From: Inspector General

Subject: Universities' Use of Social Security Numbers as Student Identifiers in Region IX
(A-09-05-15099)

OBJECTIVE

Our objective was to assess universities' use of Social Security numbers (SSN) as student identifiers and the potential risks associated with such use.

BACKGROUND

Millions of students enroll in educational institutions each year. To assist in this process, many colleges and universities use students' SSNs as personal identifiers. The American Association of Collegiate Registrars and Admissions Officers found that almost half of member institutions that responded to a 2002 survey used SSNs as the primary student identifier.¹ Although no single Federal law regulates overall use and disclosure of SSNs by colleges and universities, the *Privacy Act of 1974*, the *Family Educational Rights and Privacy Act*, and the *Social Security Act*, contain provisions that govern disclosure and use of SSNs. See Appendix A for more information on the specific provisions of these laws.

We selected two universities² from each State in Region IX.³ For each university selected, we interviewed university personnel and reviewed school policies and practices for using SSNs. See Appendices B and C for additional details regarding the scope and methodology of our review and a list of universities we contacted,

¹ *Academic Transcripts and Records: Survey of Current Practices*, April 2002 Special Report, the American Association of Collegiate Registrars and Admissions Officers.

² In this report, we use the term "universities" to refer to colleges and universities.

³ Region IX consists of the following four States: Arizona, California, Hawaii, and Nevada.

respectively. We are conducting a review in each of the Social Security Administration's (SSA) 10 regions and will issue separate reports to each Regional Commissioner.

RESULTS OF REVIEW

Based on our interviews with university personnel and reviews of school policies and practices, we are concerned about universities' use of SSNs. We identified a number of instances in which universities used SSNs as student identifiers or for other purposes. Based on prior audit and investigative work, we found that unnecessary use of SSNs increases the potential for unscrupulous individuals to illegitimately gain access to these numbers and misuse them, thus creating SSN integrity issues. Many university personnel with whom we spoke shared our concerns and have taken steps to reduce SSN use.

UNIVERSITIES' USE OF SSNs

Despite the increasing threat of identity theft, universities continued to use SSNs for a variety of purposes. We found that many universities collected students' SSNs for financial aid and tax reporting purposes. However, some universities also used the SSN for class registration, transcript requests, building access, electronic payment, and computer log-in.⁴ Other universities displayed SSNs on student identification cards, reply cards, and written examinations. This occurred, in part, because the SSN was used as the primary student identifier. Such use is unnecessary and increases the potential for fraud and abuse. Specifically, we found:

- Three universities used the SSN for access control or electronic payment. Students were assigned a magnetic stripe card (that is, swipe card) that contained their SSN to enter designated areas (such as laboratories or gymnasiums) or initiate transactions (such as making photocopies, checking out books, placing telephone calls, or purchasing meals and snacks).
- Three universities accepted students' SSNs for class registration and transcript requests. Students were allowed to register for classes and request official transcripts in paper and/or electronic format.
- Two universities printed the SSN on the student identification cards. In both instances, the SSN was used as the primary student identifier.⁵ At one university, the entire SSN was printed on the front of the student identification card. At the other university, the last six digits of the SSN were printed.

⁴ A computer log-in is used to establish communication and initiate interaction with a time-shared computer or network.

⁵ At the time of our review, these universities were issuing alternate identification numbers to their students.

- Two universities accepted students' SSNs to access computer systems. One university required the SSN to log onto computers, while it was optional at the other university. Since the SSN may be displayed, in whole or in part, on the computer monitor, the risk of disclosure to unauthorized individuals is increased.
- One university requested that prospective students provide their SSNs on reply cards used to schedule campus tours or informational meetings. These cards requested that students provide their name, address, telephone number, and other personal information, including SSN. The university plans to revise the reply cards to exclude the SSN.
- One university required that students record their SSNs on written examinations that were graded electronically. In such instances, students entered their SSN, which was used as the primary student identifier,⁶ onto Scantron sheets or Optical Mark Read forms (that is, machine-readable forms).

UNIVERSITIES AND STATES HAVE TAKEN STEPS TO LIMIT SSN USE

Some universities and States have taken steps to limit SSN use. Of the eight universities selected for review, we found that two still used the SSN as the primary student identifier. However, both universities were assigning their students alternate identification numbers. Another university did not assign specific identification numbers but, in some instances, used the SSN to distinguish between the records of students with the same name. In addition, five universities did not use the SSN as the primary student identifier. Nevertheless, one of these universities allowed its students to use the SSN in lieu of their assigned identification number. Specifically, we found:

- One university used the SSN as the primary student identifier for about 69 percent of its students as of April 2005. The university started issuing alternate identification numbers to new students in January 2005. However, for students who were enrolled before this date, the university still used the SSN as the primary identifier unless the student had requested an alternate number. The university plans to issue alternate identification numbers to all students by December 2005.
- Another university used the SSN as the primary student identifier for all students as of February 2005. However, at the time of our review, the university had initiated actions to modify its computer system and issue alternate identification numbers to current and prior students. University personnel stated these systems modifications were implemented in August 2005. As a result, the university has discontinued the use of the SSN as the primary student identifier.

⁶ See *id.*

- One university assigned unique identification numbers to all students but, as an alternative, allowed these students to use their SSN as an identifier. As a result, students could use their SSN (in lieu of their assigned nine-digit number) for identification purposes and to obtain goods and services. The university allowed students to use their SSN as an optional identifier because it was easier to remember than the assigned identification number.

In addition, both California and Arizona have enacted laws that restrict the use and disclosure of SSNs. California passed legislation that prohibits (1) publicly posting or displaying an SSN; (2) printing an SSN on any card required to access products or services; (3) requiring that an individual transmit his or her SSN over the Internet unless the connection is secure or the SSN is encrypted; (4) requiring that an individual use his or her SSN to access an Internet website, unless a password or unique personal identification number or other authentication device is also required; and (5) printing an SSN on any item mailed to an individual unless State or Federal law requires that the SSN be on the mailed document.⁷

Arizona passed legislation that prohibits those universities under the jurisdiction of the Arizona Board of Regents from assigning an identification number to faculty, staff, or students at a university that is identical to the individual's SSN. The law also prohibits the display of the SSN (or any four or more consecutive numbers of the SSN) on any Internet site maintained by the university or other publicly accessible document.⁸

Arizona also passed legislation that prohibits certain disclosures of SSNs to the public and the printing of SSNs on any card required for the individual to receive products or services. The law also establishes technical protection requirements for the on-line transmission of SSNs. In addition, the law prohibits, in certain circumstances, the printing of SSNs on mailed materials to residents of Arizona unless required by State or Federal law.⁹

Based on our interviews with university personnel, we found the two universities in California had complied with the applicable State laws to limit the use of SSNs as identifiers. However, one of the two universities in Arizona had not complied with the applicable State law that prohibits universities from assigning an identification number identical to the SSN and displaying any four or more numbers of the SSN.¹⁰ We found the university had continued to use and display the SSN as a student identifier at the

⁷ California Civil Code §§ 1798.85 and 1798.86. The restrictive provisions, in certain situations, do not become effective until January 1, 2006 or thereafter.

⁸ Arizona Revised Statutes § 15-1823.

⁹ Arizona Revised Statutes § 44-1373. The restrictive provisions, in certain situations, allow individuals and entities to continue their use of SSNs, if such use began prior to January 1, 2005.

¹⁰ Arizona Revised Statutes § 15-1823. This provision of the law became effective on June 30, 2002.

time of our review. To comply with the law, the university started issuing alternate identification numbers in January 2005 and plans to complete the process by December 2005.

POTENTIAL RISKS ASSOCIATED WITH COLLECTING AND USING SSNs

Universities' collection and use of SSNs entail certain risks, including potential identity theft and fraud. Each time an individual discloses his or her SSN, the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories, and other private information increases. Of the eight universities selected for review, there were incidences of potential SSN misuse at two universities. Because some universities still use the SSN as an identifier, students' exposure to identity theft and fraud remains. We believe the following examples illustrate students' risk of exposure to such activity.

- A student employee at a Nevada university had access to students' personal information, including names, addresses, and SSNs. The student employee allegedly obtained credit card numbers and fictitious application fees from prospective students, which were used to pay for the student employee's college expenses. University personnel were unaware of any SSN misuse. The student employee was expelled from the university.
- In California, a computer hacker gained access to one of the university's computer systems that contained the names, addresses, telephone numbers, birth dates, and SSNs of at least 600,000 individuals. The data were used by a researcher working at the university and had been obtained under authorization from a State agency.
- A laptop computer owned by a California university was stolen. The computer files contained SSNs and other personal information for about 98,000 individuals, including current, former, and prospective graduate students. The files on the laptop were downloaded by an employee for campus research and had not been encrypted.
- California authorities arrested a man suspected of stealing the names and SSNs of 150 college students and using that information to obtain credit cards and charge over \$200,000 in the students' names.

CONCLUSION AND RECOMMENDATIONS

Despite the potential risks for SSN misuse and identity theft, some universities continue using SSNs as student identifiers or for other purposes. While we recognize SSA cannot prohibit universities from using SSNs as student identifiers, we believe SSA can help reduce potential threats to SSN integrity by encouraging universities to limit SSN collection and use. We also recognize the challenge of educating such a large number of educational institutions about unnecessary SSN use. However, given the potential threats to SSN integrity, such a challenge should not discourage SSA from taking steps to safeguard SSNs. Accordingly, we recommend that SSA:

1. Coordinate with universities and State/regional educational associations to educate the university community about the potential risks associated with using SSNs.
2. Encourage universities to limit their collection and use of SSNs.
3. Promote the best practices of educational institutions that no longer use SSNs as student identifiers.

AGENCY COMMENTS

SSA agreed with all of our recommendations. See Appendix D for the text of SSA's comments.



Patrick P. O'Carroll, Jr.

Appendices

[APPENDIX A](#) – Federal Laws that Govern Disclosure and Use of the Social Security Number

[APPENDIX B](#) – Scope and Methodology

[APPENDIX C](#) – Educational Institutions Contacted

[APPENDIX D](#) – Agency Comments

[APPENDIX E](#) – OIG Contacts and Staff Acknowledgments

Federal Laws that Govern Disclosure and Use of the Social Security Number

The following Federal laws establish a general framework for disclosing and using the Social Security number (SSN).

The Privacy Act of 1974 (5 U.S.C. § 552a; Pub. L. No. 93-579, §§ 7(a) and 7(b))

The *Privacy Act of 1974* provides that it is unlawful for a State government agency to deny any person a right, benefit, or privilege provided by law based on the individual's refusal to disclose his/her SSN, unless such disclosure was required to verify the individual's identity under a statute or regulation in effect before January 1, 1975. Further, under *Section 7(b)*, a State agency requesting that an individual disclose his/her SSN must inform the individual whether the disclosure is voluntary or mandatory, by what statutory or other authority the SSN is solicited and what uses will be made of the SSN.

The Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99)

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. FERPA applies to those schools that receive funds under an applicable program of the U.S. Department of Education. Under FERPA, an educational institution must have written permission from the parent or eligible student to release any personally identifiable information (which includes SSNs) from a student's education record.¹ FERPA does, however, provide certain exceptions in which a school is allowed to disclose records without consent. These exceptions include disclosure without consent to university personnel internally who have a legitimate educational interest in the information, to officials of institutions where the student is seeking to enroll/transfer, to parties to whom the student is applying for financial aid, to the parent of a dependent student, to appropriate parties in compliance with a judicial order or lawfully issued subpoena, or in the event of a health or safety emergency.

¹ FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the child when the child reaches age 18 or attends an institution of postsecondary education. Children that have been transferred rights are referred to as "eligible students."

The Social Security Act

The Social Security Act provides that “[s]ocial security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such Social Security account number or related record.” (42 U.S.C. § 405(c)(2)(C)(viii)). The Social Security Act also provides that “[w]hoever discloses, uses, or compels the disclosure of the Social Security number of any person in violation of the laws of the United States; shall be guilty of a felony...” (42 U.S.C. § 408(a)(8)).

Scope and Methodology

To accomplish our objective, we:

- interviewed selected university personnel responsible for student admissions/registrations;
- reviewed Internet websites of eight colleges and universities we contacted;
- reviewed applicable laws and regulations; and
- reviewed selected studies, articles, and reports regarding universities' use of Social Security numbers (SSN) as student identifiers.

We visited five educational institutions and interviewed personnel at three others to learn more about their policies and practices for using SSNs as student identifiers. Our review of internal controls was limited to gaining an understanding of universities' policies over the collection, protection and use or disclosure of SSNs. The Social Security Administration entity reviewed was the Office of the Deputy Commissioner for Operations. We conducted our audit from February through August 2005 in accordance with generally accepted government auditing standards.

Educational Institutions Contacted

We interviewed personnel at eight educational institutions in Region IX. The following table shows the names and locations of these schools as well as their approximate student enrollments.

	School	Location	Student Enrollment
1	Arizona State University	Tempe, Arizona	58,156
2	University of California, Berkeley	Berkeley, California	31,676
3	San Francisco State University	San Francisco, California	28,804
4	University of Nevada, Las Vegas	Las Vegas, Nevada	27,000
5	Hawaii Pacific University	Honolulu, Hawaii	9,000
6	Chaminade University	Honolulu, Hawaii	2,800
7	Prescott College	Prescott, Arizona	1,036
8	University of Southern Nevada	Henderson, Nevada	300

Source: We determined student enrollment by reviewing university websites.

Agency Comments



SOCIAL SECURITY

MEMORANDUM

Date: NOV 16 2005

Refer To: S2D9B52

To: Inspector General

From: Regional Commissioner
San Francisco

Subject: Universities' Use of Social Security Numbers as Student Identifiers in Region IX
(A-09-05-15099)

Thank you for the opportunity to review the draft report. We share your concern over the dangers of identity theft raised by collection, use and display of the Social Security Number (SSN) by schools, and are encouraged to learn that California and Arizona, at least, have taken measures to address this problem through State law. We support your recommendation that SSA undertake outreach activities to the university community to reduce unnecessary use of the SSN.

If you would like to discuss this further, please feel free to call me at (510) 970-8400. Staff questions may be directed to Alan Follett on our Retirement and Survivors Insurance Team at (510) 970-8245.


Peter D. Spencer

OIG Contacts and Staff Acknowledgments

OIG Contacts

James J. Klein, Director, (510) 970-1739

Jack H. Trudel, Audit Manager, (510) 970-1733

Acknowledgments

In addition to those named above:

Regina Finley, Auditor-in-Charge

James Sippel, Senior Auditor

Kimberly Beauchamp, Writer-Editor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-09-05-15099.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Executive Operations (OEO). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Executive Operations

OEO supports OIG by providing information resource management and systems security. OEO also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OEO is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.