
**OFFICE OF
THE INSPECTOR GENERAL**

SOCIAL SECURITY ADMINISTRATION

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

August 2005

A-06-05-15100

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: August 19, 2005

Refer To:

To: Ramona Schuenemeyer
Regional Commissioner
Dallas

From: Inspector General

Subject: Universities' Use of Social Security Numbers as Student Identifiers in Region VI
(A-06-05-15100)

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, in response to a 2002 survey, half of member institutions used SSNs as the primary student identifier.¹ Although no single Federal law regulates overall use and disclosure of SSNs by universities,² the *Privacy Act of 1974*, the *Family Educational Rights and Privacy Act* (FERPA), 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 a sample of 10 universities consisting of 2 universities from each of 5 States³ in the Dallas Region. At each university, we interviewed appropriate personnel and reviewed university policies and practices concerning the use of SSNs. Appendices B and C provide additional details regarding the scope and methodology of our review and a list of the universities we contacted. 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.

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

² The term "universities" will be used to include both colleges and universities.

³ Arkansas, Louisiana, New Mexico, Oklahoma, and Texas.

RESULTS OF REVIEW

All 10 universities selected for review in the Dallas Region used the SSN as their primary student identifier. However, 7 of the 10 universities indicated they were implementing a new system in 2005 to limit the use of the SSN as the primary student identifier. Personnel at the remaining three universities informed us they also planned to implement a new system: one in January 2006; one within 2 years; and one within 3-5 years. All five States within our region had taken steps to address identity theft or limit the use and display of SSNs.

UNIVERSITIES' USE OF SSNs

The universities used the SSN for admission applications, class registration, access to computer systems, class rosters, grade or transcript reports, student identification (ID) cards and student financial aid. During our review, we noted that 1 of the 10 universities displayed the full SSN on the face of the student ID card, and 1 displayed the last 4 digits of the SSN. Both universities planned to change their system to use another number in place of the SSN. The other eight universities did not use the SSN on the front of their student ID cards. In addition, seven of the universities included the SSN in a magnetic strip or bar code on the back of the student ID card, but all 10 had plans to discontinue this practice when they implement their new systems.

All of the universities contacted originally used SSNs for various purposes because the SSN was universally accepted as a standard form of identification; the SSN met Federal reporting requirements for student financial aid; or State government required the SSN. At the time of our review, 7 of the 10 universities used the SSN for on-line applications, and 9 of the 10 universities used the SSN to post grades. However, the grades were posted on-line, and the instructors were told not to post them publicly. All of the universities expressed concern about the growing trend of identity theft and SSN misuse. All 10 universities stated they used a variety of system security measures to secure their on-line transactions, including personal identification numbers, passwords, firewalls and encryption.

We also identified instances in which universities requested that prospective students provide their SSNs on postcards. Universities routinely send postcards to be completed by prospective students who have requested information about the university. These postcards request name, address, graduation information, and the prospective student's SSN. Displaying such information on a postcard increases the risk of SSN misuse and unnecessarily subjects the prospective student to the possibility of identity theft. At the time of our review, 3 of the 10 universities requested the student's SSN on information request postcards. Of those universities, one placed "optional" next to the SSN request. Below is an example of an information request postcard.

INFORMATION REQUEST CARD			
Name _____ <i>Last</i>	<i>First</i>	<i>M.I.</i>	<i>Preferred Name</i>
Address _____			
City _____	State _____	Zip _____	
Social Security No. (optional) _____			
E-mail _____	Phone _____		
Date of Birth _____	Sex <input type="checkbox"/> F <input type="checkbox"/> M		
Intended Major/Area of Interest _____			
High School Attending _____		Year of Graduation _____	
Please send me more information on: <input type="checkbox"/> Financial Aid <input type="checkbox"/> Scholarships <input type="checkbox"/> Housing			
<input type="checkbox"/> Student Life <input type="checkbox"/> Other _____			

STATES AND UNIVERSITIES LIMIT SSN USE

All five States in the Dallas region have current or pending legislation to address identity theft or limit the use and display of SSNs. Additionally, all 10 of the universities contacted reported taking steps or making plans to limit using SSNs as the primary student identifier.

States' Efforts to Limit SSN Use

Among the current or pending laws in the States:

- Arkansas has a law that makes it a crime for an individual without consent, to obtain or record identifying information of another person that would assist in accessing the financial resources of that person. The law includes SSNs in its definition of "identifying information." (A.C.A. § 5-37-227).
- Louisiana has a law that prohibits the use of SSNs as personal identifiers for school employees. (La. R.S. 17:440).

- New Mexico has legislation pending that increases the penalty for identity theft for “...willfully obtaining, recording or transferring personal identifying information of another person without the authorization or consent of that person and with the intent to defraud that person or another.” (2005 Bill Text NM S.B. 260).
- Oklahoma has a law that makes it a crime “...for any person to willfully and with fraudulent intent to obtain the name, address, social security number, date of birth...or any other personal identifying information of another person living or dead, with intent to use, sell, or allow any other person to use or sell such personal information to obtain or attempt to obtain money, credit, goods, property, or service in the name of the other person without the consent of that person.” (21 Okla. St. § 15331.1).
- Texas has a law that prohibits the printing of “...an individual’s social security number on a card or other device required to access a product or service...unless the individual has requested in writing such printing.” The law does not apply to “...the collection, use, or release of a social security number that is required by state or federal law...or the use of a social security number for internal verification or administrative purposes.” (Tex. Bus. & Com. Code § 35.58).

Universities’ Efforts to Limit SSN Use

All 10 universities we contacted reported taking steps or making plans to limit using SSNs as the primary student identifier. All 10 universities gave students the option of using another number as a personal identifier and addressed privacy of student records via FERPA or through discussion in university catalogs or on websites. One university had a statement on the admission application regarding the State’s Public Information Act, and another university had information on its website explaining the new student identification numbering system.

While conducting our review, we also noted articles in student publications outlining concerns and possible solutions to identity theft and an article at another university entitled *Old ID Cards hold SSN, new card effective mid – March*. This is an example of the university taking action and informing students, faculty and staff about their new student identifier system.

Overall, we are encouraged that officials from the universities we contacted shared our concerns and stated their universities had taken, or were planning to take, steps to reduce using the SSN as the primary identifier. Most significantly, 7 of the 10 planned to implement a new student identifier system with implementation dates ranging from March to October 2005. The new systems will limit the use of SSNs as the primary student identifier.

POTENTIAL RISKS ASSOCIATED WITH USING SSNs AS STUDENT IDENTIFIERS

Universities' use of SSNs as primary identification numbers entails certain risks, including potential identity theft and fraud. Each time an individual divulges his or her SSN, he or she is exposed to having the number stolen and used for unintended purposes. The exposure to identity theft increases when the SSN is the student identification number. It is important for universities, as well as individuals, to help prevent identity theft and fraud to the extent possible by reducing this exposure. The following examples illustrate students' risk of exposure to identity theft and fraud.

- A university professor in Washington was indicted on 33 counts of mail fraud in a scam using students' SSNs. The professor allegedly accessed the university's records system and used students' information to obtain new SSN cards by posing as a parent. The professor then allegedly used the SSNs to obtain credit cards and birth certificates.
- 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.
- A New York school notified about 1,800 students that their SSNs and other personal information had been posted on a university website. The university shut down the website.
- A student at a Texas university was indicted for hacking into the school's computer network and downloading the names and SSNs of over 37,000 students, faculty, and alumni.
- An individual discovered a computer printout in a trash bin near a Pennsylvania university listing SSNs and other personal data for hundreds of students.

CONCLUSION AND RECOMMENDATIONS

All 10 universities we contacted in the Dallas Region used the SSN as the primary student identifier, but 7 indicated they were implementing a new system in 2005. The remaining three planned to implement a new system after 2005. While the universities continue to use the SSN as the primary student identifier, there is a continuing inherent risk that personal information could be compromised and potentially misused. While we recognize that SSA cannot prohibit universities from using SSNs as student identifiers, we believe SSA has a responsibility to 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. 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 as student identifiers.
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

In commenting on our draft report, SSA agreed with our recommendations. The Regional Commissioner also suggested that SSA's Central Office establish a dialogue with national educational organizations to promote the best practices of educational institutions that do not use the SSN as a student identifier.

OIG RESPONSE

Establishing a dialogue with national educational organizations would provide SSA an effective method of communicating the best practices of educational institutions that do not use the SSN as a student identifier. Accordingly, we encourage the Regional Commissioner to work with the Central Office to open these lines of communication.

OTHER MATTER

While conducting our survey work, we identified several instructors' resumes that contained SSNs, dates of birth, birthplaces, home telephone numbers, and addresses on a website for a university in Texas. Because of the growing prevalence of identity theft, we believe that, when SSA contacts the universities and staff, it should remind them to (1) issue periodic reminders to students and faculty about safeguarding their SSNs and (2) conduct periodic reviews to ensure SSNs are not inadvertently placed on their websites.



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

Appendix A

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 universities 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 university 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 to health care providers 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 the age of 18 or attends an institution of postsecondary education. Children that have been transferred these rights are referred to as "eligible students."

The Social Security Act

The Social Security Act provides that “Social 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

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

To accomplish our objective, we:

- reviewed applicable laws and regulations;
- reviewed selected studies, articles and reports regarding universities' use of Social Security numbers (SSN) as student identifiers;
- selected 2 universities from each of the 5 States in the Dallas Region;
- reviewed Internet websites for all 10 universities selected for our review;
- visited 7 universities and conducted telephone interviews at 3 others to learn more about their policies and practices for using SSNs as student identifiers; and
- interviewed selected university personnel responsible for student admissions/registrations.

Our review of internal controls was limited to gaining an understanding of universities' policies over the collection, protection and use/disclosure of SSNs. The Social Security Administration office responsible for SSN issues was the Office of the Deputy Commissioner for Operations. We conducted our audit from January through March 2005 in accordance with generally accepted government auditing standards.

Appendix C

Educational Institutions Contacted

We interviewed personnel at 10 educational institutions in Region VI. The following table shows the names and locations of these universities as well as their total student enrollments.

	University	Location	Student Enrollment
1	Louisiana State University and Agriculture and Mechanical College	Baton Rouge, Louisiana	30,211
2	University of Oklahoma	Norman, Oklahoma	24,946
3	University of New Mexico	Albuquerque, New Mexico	24,217
4	Collin County Community College	Plano, Texas	15,985
5	Texas Woman's University	Denton, Texas	10,714
6	Northeastern State University	Tahlequah, Oklahoma	9,454
7	University of Arkansas at Little Rock	Little Rock, Arkansas	9,330
8	Arkansas Tech University	Russellville, Arkansas	6,359
9	Louisiana State University in Shreveport	Shreveport, Louisiana	4,316
10	Santa Fe Community College	Santa Fe, New Mexico	1,450

Source: We determined student enrollment by reviewing university websites or the following website:
www.collegeboard.com

Agency Comments

Date: August 2, 2005

To: Inspector General

From: Regional Commissioner
Dallas

Subject: Review of Universities' Use of Social Security Numbers as Student Identifiers in Region VI, Audit No. 22005026

We appreciate the opportunity to review and comment on the draft report "Universities' Use of Social Security Numbers as Student Identifiers" (A-06-05-15100). We have the following comments on the recommendations:

Recommendation 1:

Coordinate with universities and State/regional educational associations to educate the university community about the potential risks associated with using SSNs as student identifiers.

Comments: As our managers and public affairs specialists continue their regular and ongoing contacts at colleges and universities, we will ask them to stress the potential risks associated with using SSNs as student identifiers. We would appreciate any State/regional educational association names and contact information that OIG may have identified during this audit to ensure that all appropriate contacts are made.

Recommendation 2:

Encourage universities to limit their collection and use of SSNs.

Comments: As our managers and public affairs specialists continue their regular and ongoing contacts with educational institutions, we will ask that they encourage them to limit the collection and use of SSNs. We will also suggest they consider: (1) issuing periodic reminders to students and faculty about safeguarding their SSNs; and (2) conducting periodic reviews to ensure SSNs are not inadvertently placed on their websites.

We will specifically contact the university in Texas identified during your study as having a website where several instructors' resumes with identifying information and SSNs were found, and alert the university to the risks of such practices.

Recommendation 3:

Promote the best practices of educational institutions that no longer use SSNs as student identifiers.

Comments: We agree that coordination and promotion of educational institutions' best practices would be in our best interest. However, we believe that such efforts would be better served at the national level with SSA Central Office working with the national educational organizations to set up this dialogue and/or website.

If members of your staff have questions, please have them call Vickie Higgins at 214-76-2165 in Management and Operations Support, Center for Programs Support.

/s/

Ramona Schuenemeyer

Appendix E

OIG Contacts and Staff Acknowledgments

OIG Contacts

Paul Davila, Director, (214) 767-6317

Paul Wood, Audit Manager, (214) 767-0058

Acknowledgments

In addition to those named above:

Billy Mize, Senior Auditor

For additional copies of this report, please visit our web site at www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-06-05-15100.

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.