SOCIAL SECURITY
Office of the Inspector General

October 3, 2001

The Honorable Charles E. Grassley
Ranking Minority Member
Committee on Finance
United States Senate
Washington, D.C. 20510

Dear Senator Grassley:

In response to your August 6, 2001 letter to Acting Commissioner Massanari and myself, the Social Security Administration (SSA), Office of the Inspector General is pleased to provide you with the requested information related to Social Security number (SSN) misuse.

As you are aware, my office is charged with preventing and detecting fraud, waste and abuse in Social Security programs and operations. Because the misuse of an SSN falls within that mandate, we are well acquainted with the SSN misuse and identity theft phenomena. In recent years, as these phenomena have grown exponentially, we have worked with SSA, Congress, other Government entities, as well as the public, to stem the tide of SSN misuse and, if one is optimistically inclined, begin a trend in the opposite direction. Nevertheless, we recognize that much work needs to be done within SSA, and some very difficult decisions will have to be made by Congress before we can make meaningful headway in the war against SSN misuse.

In responding to most of the questions you posed, we relied on information developed in past audits, evaluations and investigations. For the remaining questions, we obtained data through interviews of SSA representatives and analysis of information provided by these sources.

The enclosed report contains our insights and conclusions regarding the following subjects:

- Assignment and issuance of SSNs,
- Undeliverable SSN cards,
- Earnings records and the Earnings Suspense File,
- Programs/operations with the most incidences of SSN misuse,
- Employee SSN misuse cases,
- Proper use and dissemination of the SSN,

- Coordination with other Federal agencies,
- Preventative measures to stop SSN misuse, and
- Data matching efforts.

If you have any questions or would like to be briefed on this issue, please call me or have your staff contact Richard A. Rohde, Special Agent-in-Charge for External Affairs, at (410) 966-1722.

Sincerely,

James G. Huse, Jr.
Inspector General of Social Security

Enclosure

CONGRESSIONAL RESPONSE REPORT

SSN Misuse: A Challenge For the Social Security Administration

A-08-02-22030

OCTOBER 2001

Background

In 1935, the Social Security Act authorized the creation of the Social Security number (SSN) as part of a new system to track the earnings of employed Americans. Despite the narrowly drawn purpose of this nine-digit number, use of the SSN as a general identifier in record systems eventually grew. In 1967, the Department of Defense abandoned the military identification number in favor of the SSN for armed forces personnel. In the 34 years since, the myriad uses of the SSN have continued to expand.

Misuse of the SSN, catalyzed by the Internet, has quickly become a national dilemma. The SSN's universality has become its own worst enemy. The power it wields—power to engage in financial transactions, power to obtain personal information, power to create or commandeer identities—makes it a valuable asset and one that is subject to limitless abuse. For example, in Fiscal Year (FY) 2000, the Office of the Inspector General (OIG) received 92,847 allegations of fraud, waste, or abuse. Over half of these, 46,840, were allegations of SSN misuse, and another 43,456 were allegations of program fraud, which experience has shown often includes implications of SSN misuse.

Results of Review

On August 6, 2001, Senator Charles E. Grassley, Ranking Member, Senate Finance Committee, issued a letter to the Acting Commissioner of Social Security and the Inspector General of the Social Security Administration (SSA.) In this letter, Senator Grassley requested that SSA and the OIG conduct independent assessments of "SSA's programs and operations with the goal of minimizing opportunities for SSN misuse at its administrative core." Senator Grassley specifically requested that the two organizations provide assessments of nine distinct elements. These elements and OIG's insights and conclusions follow.

1. Evaluate Whether SSA's Enumeration Business Process is Sufficient to Ensure the Proper Assignment and Issuance of SSNs.

Over the past several years, SSA's OIG has issued numerous reports in which we highlighted certain vulnerabilities within the Agency's enumeration business process that allow the improper assignment of SSNs. We are confident SSA has given careful consideration to these vulnerabilities and, to its credit, has expeditiously implemented many of the recommendations made in our reports. However, there are a number of recommendations that the Agency disagreed with or that have yet to be implemented. As a result, we believe there are still vulnerabilities within the enumeration system that allow the improper assignment and issuance of SSNs. We believe the following areas continue to be weaknesses in SSA's enumeration process.

EVIDENTIARY DOCUMENTS PRESENTED WITH SSN APPLICATIONS

When an individual applies for an original SSN, SSA requires the applicant to provide acceptable documentary evidence of *age, identity,* and *United States citizenship or lawful alien status.* When applying for a replacement SSN, the applicant must provide evidence of *identity* and, if applicable, *lawful alien status.* Reliable evidentiary documentation is crucial to ensuring the proper assignment of SSNs. Unfortunately, given the technological advances in today's society, motivated individuals can counterfeit official documents with surprising accuracy. In fact, through our audits, evaluations and investigations, we have detected SSNs issued to individuals based on counterfeit evidentiary documents.

To effectively foil the efforts of these individuals and reduce the occurrences of improper SSN attainment, we recommended that SSA employ effective front-end controls in its enumeration process. The Agency accepted many of these recommendations and has initiated, or is in the implementation planning process for, most of our proposed corrective actions. However, SSA elected not to implement one recommendation that it believed would be administratively burdensome and negatively impact customer service.

Specifically, we recommended that SSA obtain independent verification from the issuing Agency (e.g., Immigration and Naturalization Service (INS), State Department) for all evidentiary documents submitted by noncitizens before issuing an original SSN. Our audits, evaluations and investigations have indicated that documents presented by some noncitizens are problematic. Additionally, we concluded SSA's current verification process is not sufficient to ensure the validity of evidentiary documents presented by noncitizens. For example, in one audit, we found that 999 of the 3,557 original SSN applications reviewed were approved based on improper evidentiary documentation.[1] We acknowledge that this is not the case with the majority of noncitizen documents. However, our experience has shown that the error rate is significant enough to warrant increased verification of these documents.

SSA is working with INS and the State Department on a program that would provide for the enumeration of noncitizens at the port of entry ("Enumeration at Entry" program). We believe that this program will be extremely beneficial once fully implemented. However, we are concerned that full implementation could be years away. We continue to believe SSA should not issue SSNs until evidentiary evidence submitted by noncitizens has been validated**.** This recommendation is essential, not only to prevent SSN misuse and identity theft, but to help ensure that unauthorized noncitizens do not readily assimilate themselves in everyday American life with an improperly obtained SSN.

CONTROLS WITHIN SSA'S MODERNIZED ENUMERATION SYSTEM

SSA's assignment of an SSN is dependent on the processing of SSN applications through SSA's Modernized Enumeration System (MES). When an application is entered in MES, the program processes the information and performs various automated edits including a determination of whether the applicant has previously obtained an SSN. If these edits are passed, the system assigns an SSN and a card is issued to the applicant.

Through previous audit work, we determined that edits within MES could be enhanced to provide more reliable results. For example, in a recent audit, we identified instances in just 4 States in which SSA assigned multiple SSNs to 178 infants. These instances occurred because MES edits did not recognize the applications as duplicate.[2] In many of these cases, only one or two letters were different in the applicants' name.

In addition to enhancing existing edits, we have recommended that SSA incorporate preventive controls in MES to stop the assignment and issuance of SSNs when the system detects the following occurrences.

---

[1] SSA/OIG report entitled *Procedures for Verifying Evidentiary Documents Submitted With Original Social Security Number Applications*, September 2000 (A-08-98-41009).

[2] SSA/OIG report entitled *Review of Enumeration at Birth Program*, September 2001 (A-08-00-10047).

- Over a specified period of time, SSA issued multiple SSNs cards to the same address.

- Over a specified period of time, parents claimed to have had an unusually large number of children.

- Known fraudulent documentation is presented as evidence in support of an SSN application.

Current edits addressing these issues concentrate on the detection of fraud after it has already occurred. Unfortunately, once an SSN has been issued, SSA has little ability to prevent or curtail the use of that SSN in committing further fraud. Accordingly, SSA is in the process of incorporating some of these edits in MES. However, full implementation may take several years. We believe that these enhancements should be accelerated and that if funding is an issue the Agency should identify the resource requirements.

LIMITATIONS ON THE NUMBER OF REPLACEMENT SSN CARDS OBTAINED

Because many cases of identity fraud involve improperly obtained replacement cards, we believe SSA needs to develop a combination of regulations and system controls to limit the number of replacement SSN cards an individual can receive during a specified period. In a recent audit, we determined that 192 individuals obtained 6 or more replacement SSN cards during a 1-year period.[3] Through examination, we concluded that over 100 of these individuals appeared to be misusing their SSNs. Under current SSA policy, any individual can obtain up to 52 replacement SSN cards in a year. Although we recognize there could be extraordinary occurrences in which an individual might have a need for several SSN cards, we believe this should be the exception. Accordingly, we believe SSA should establish a reasonable threshold for the number of replacement SSN cards an individual may obtain during a year and over a lifetime. SSA should then implement controls within its system requiring management personnel to approve any applications exceeding this limit.

TRAINING AND QUALITY REVIEWS FOR SSA EMPLOYEES

Well-trained employees are as important to the enumeration process as procedures and systems. Based on recent audits, we believe SSA field office employees would benefit from educational reinforcement through training and quality reviews of SSN processing. Specifically, we have recommended that SSA should:

- Re-emphasize the importance of following enumeration policies and procedures associated with the issuance of original and replacement SSN cards, including the

[3] SSA/OIG report entitled *Replacement Social Security Number Cards: Opportunities to Reduce the Risk of Improper Attainment and Misuse*, September 2001 (A-08-00-10061.)

requirement to independently verify INS documents when indicated by SSA policy and the Systematic Alien Verification for Entitlements (SAVE) program.[4]

- Conduct periodic quality reviews of processed SSN applications and provide timely feedback to field office personnel.[5]

- Test field office employee compliance with procedures for issuing replacement SSN cards when performing periodic enumeration quality reviews. Additional training and/or supervision should be provided to employees if necessary.[6]

- Instruct field office personnel to exercise greater care when resolving enumeration feedback messages generated by the system.[7]

- Require field office personnel to document the basis of all resolution actions taken on enumeration feedback messages for an appropriate period of time to facilitate management review.[8]

- Require FO management to perform periodic quality reviews of processed enumeration feedback messages and provide appropriate feedback and related training to FO personnel.[9]

2. Determine How Many SSNs SSA Cannot Account For in the Past Five (5) Years, and Evaluate How SSA Can Improve Its Accounting Methods in the Future.

Because we have performed no audit work in this area, we defer to SSA on this question.

Our FY 2002 Annual Audit Plan does include an assignment to determine whether adequate security and controls exist for the mailing of SSN cards. Preliminary research indicates that SSA does not track the number of SSN cards returned to the Agency as undeliverable. Rather, the returned cards are kept in a secure container in the

---

[4] SSA/OIG report entitled *Replacement Social Security Number Cards: Opportunities to Reduce the Risk of Improper Attainment and Misuse*, September 2001 (A-08-00-10061.)

[5] SSA/OIG report entitled *Review of Controls over Nonwork Social Security Numbers*, September 1999 (A-08-97-41002).

[6] SSA/OIG report entitled *Replacement Social Security Number Cards: Opportunities to Reduce the Risk of Improper Attainment and Misuse*, September 2001 (A-08-00-10061.)

[7] SSA/OIG report Effectiveness of Internal Controls in the Modernized Enumeration System, September 2000 (A-08-97-41003).

[8] SSA/OIG report *Effectiveness of Internal Controls in the Modernized Enumeration System*, September 2000 (A-08-97-41003).

[9] SSA/OIG report *Effectiveness of Internal Controls in the Modernized Enumeration System*, September 2000 (A-08-97-41003).

mailroom and periodically destroyed. An SSA Office of Management and Operations Support staff member estimated that the number of returned cards ranges between 250,000 and 500,000 per year. Accordingly, in the pursuant audit report, we will make recommendations, as necessary, to improve methods of accounting for returned SSN cards in the future.

3. Evaluate How Well SSA Maintains Accurate Earnings Records For Individuals.

SSA has reported it is able to correctly post over 99 percent of all wage reports it receives to the appropriate earner's record. However, approximately one percent of the wages submitted by employers fail the name/SSN validation criteria within SSA's systems and are therefore posted to the Earnings Suspense File (ESF). Between 1937 and 1999, the ESF grew to about 227 million reports of individual earnings with a value of about $333 billion. We have reported our concerns related to the ESF's impact on benefit amounts and the added administrative costs related to correcting invalid earnings information. In addition, the ESF is indicative of a nationwide problem of potential fraud and misuse that not only affects SSA programs but transcends to other Federal entities, such as the Internal Revenue Service (IRS) and INS.

In earlier reports, SSA OIG reported some of the weaknesses in the current earnings reporting process, such as significant suspended wages, duplicate postings, and poor controls over employer wage reporting. For example, we reported that SSA's ESF represents a major management challenge because it continues to grow in size each year.[10] SSA developed a Tactical Plan containing an overall strategy and several individual projects designed to reduce the ESF's rate of growth and size. However, the changes called for in the Plan are long-term, and several factors, both internal and external to SSA, hinder the efforts with the most potential to reduce the ESF's size and growth. Some of the internal factors hindering efforts to reduce the ESF's size include: (1) SSA has placed a higher priority on other automated systems developments and (2) SSA has not linked available information in its data base to identify chronic "problem" employers who continually submit annual wage reports with multiple errors. External factors include other Federal agencies with separate yet related mandates, such as the IRS' reluctance to sanction employers for submitting invalid wage data[11] and INS' complicated employer procedures for verification of eligible employees.

In terms of duplicate postings, an earlier OIG audit found that the Master Earnings File contained more than $8.3 billion in duplicate earnings postings.[12] These earnings errors

[10] SSA/OIG report entitled *The Social Security Administration's Earnings Suspense File Tactical Plan and Efforts to Reduce the File's Growth and Size*, February 2000 (A-03-97-31003).

[11] Under IRS code 26 U.S.C. §6721 (a), the IRS may charge a $50 penalty each time an employer does not furnish an employee's correct SSN on a wage report.

[12] Department of Health and Human Services OIG report entitled *Controls Over Duplicate Postings of Self-Employment Income to the Master Earnings Record*, August 1993 (A-13-92-00228).

caused over $10.5 million in excess payments to about 31,800 beneficiaries. Another OIG audit found that SSA did not maintain sufficient controls over the wage reporting process to ensure employers were submitting quality earnings data.[13] The audit noted how 285 employers submitted erroneous wage reports, where more than 50 percent of their wages were in error, for 3 years in a row without SSA taking any action, even though more than $8.5 million in penalties could have been assessed. Another 3,428 employers submitted similar erroneous wage reports for 2 years in a row.

4. Determine Which SSA Programs and Operations Have the Most Incidences of SSN Misuse.

It is difficult to definitively conclude which SSA programs or operations have the most incidences of SSN misuse since it is impossible for OIG to verify the legitimacy of every allegation received. With limited staff and an overwhelming number of allegations, OIG's Office of Investigations (OI) prioritizes the cases it can feasibly examine. Our first priority has traditionally been to investigate cases involving possible employee fraud. Secondly, we attempt to examine the large volume of programmatic cases that negatively impact Social Security trust funds. Accordingly, we are only able to provide statistics based on the SSN misuse cases our investigators have closed. We acknowledge that this representation may not be reflective of the total crimes that have occurred. However, given our mandate of attempting to secure SSA's trust fund dollars, these figures reflect the cases our established priorities and current resource level allowed us to pursue.

During the past 5 fiscal years, the percentage of the cases involving SSN misuse and program fraud are as follows:

Program Category	Percent of Closed SSN Misuse Cases Involving SSA Program Losses
Title XVI – Aged Supplemental Security Income (SSI)	41.6
Title II – Disability	25.9
Title II – Retirement, Survivors Insurance (RSI)	19.8
Title XVI – Disability (SSI)	11.0
Concurrent (Title II and Title XVI)	1.5

Title XVI – Aged SSI is the program for persons 65 years of age or older who demonstrate a financial need for assistance as mandated by law and program requirements. As shown in the chart above, title XVI – Aged SSI cases accounted for the majority of closed cases for which SSN misuse was also involved. Additionally, a measurable percent of SSN misuse cases involved losses to the title II Disability and

[13] SSA/OIG report entitled *Force Processing of Magnetic Media Wage Reports with Validation Problems*, May 2001 (A-03-99-31001).

RSI programs. We have included an example case for each program category below to provide an understanding of how SSN misuse impacted these cases.

Title XVI – Aged SSI Recipient Used Three Aliases to Collect Benefits

On May 21, 2001, before the honorable U.S. District Court Judge Robert J. Timlin, Ms. Jean M. Whiteley (84 years old) was sentenced to 6 months home detention, 5 years probation, 60 hours of community service, a $300 special assessment fee and ordered to repay SSA $423,845.

The OIG initiated an investigation of Ms. Whiteley in September 1999, based on a referral from an SSA Assistant District Manager (ADM). The ADM informed OIG that, as a result of a joint project between SSA and the California Department of Health Services, the Palm Springs SSA office determined Ms. Whiteley had fraudulently collected SSA benefits under more than one identity. Additional investigation by the OIG revealed that Ms. Whiteley had been receiving SSA Widows' Insurance Benefits (WIB) under the alias of Anna K. Whiteley since 1981, SSI benefits under the alias Ann Jeanette Oliver since 1982 and SSI benefits under the alias of Jean L. Whiteley since 1987. The investigation also revealed that since 1988, Ms. Whiteley received SSI benefits (aged) on her deceased husband's fraudulent identity.

On November 9, 1999, OIG Special Agents executed a Federal search warrant at Ms. Whiteley's residence in Desert Hot Springs, California. Items seized pursuant to the search warrant indicated that Ms. Whiteley used the aforementioned aliases to fraudulently receive SSA WIB and SSI benefits. In addition, items seized indicated that she used the aliases to fraudulently apply for Federal bankruptcies, California State Renter's Tax Credits, County Home Energy Assistance and Rural Housing Assistance from the U.S. Department of Agriculture.

On January 28, 2000, a Federal Grand Jury returned a fourteen-count felony indictment for Ms. Whiteley in U.S. District Court, Los Angeles, California. Ms. Whiteley was indicted on twelve counts of 18 U.S.C. § 1343, "Fraud by wire, radio, or television." Additionally, she was indicted on two counts of 18 U.S.C. § 152, "Concealment of assets; false oaths and claims; bribery." Subsequently, she pled guilty to three counts of the aforementioned.

The loss to SSA from her crimes totaled approximately $423,845. Additional losses to the Federal government from fraudulent bankruptcy filings equal approximately $160,000.00.

Title II Disability Recipient Used Father's and Daughter's SSNs to Conceal Work Activity

On January 10, 2001, Mr. Anthony P. Coco was sentenced in Federal District Court by the Honorable Judge Clarence Newcomer to serve 5 months in prison followed by 5 months home detention. Following his release from prison, Mr. Coco will serve 3 years probation. Additionally, Judge Newcomer ordered Mr. Coco to repay $115,541 in restitution to SSA. Mr. Coco was further ordered to pay

all costs of electronic monitoring related to his home detention. Mr. Coco voluntarily surrendered himself to the U.S. Bureau of Prisons on January 29, 2001 to begin his prison sentence.

Mr. Coco became entitled to receive title II disability benefits in 1985. However, from 1986 to 1999, Mr. Coco used his father's and daughter's SSNs to conceal his own work activity while still collecting disability benefits under his own SSN.

Title II RSI Recipient Used Deceased Brother's Identity

On May 23, 2001, Mr. Peter Collins appeared in the U.S. District Court for the Northern District of Ohio for the purpose of sentencing. Mr. Collins had previously pled guilty to one count of violating 18 U.S.C. § 641, "Public money, property or records" in this same court. Judge Peter Economus sentenced Mr. Collins to a period of 6 months' home confinement and 3 years' probation. Collins was also fined $1,100 and ordered to make restitution in the amount of $28,243 to SSA.

This case was initiated when the North Olmsted, Ohio Police Department discovered that Mr. Collins had two Ohio Driver Licenses listing two separate SSNs. One of the SSNs was assigned to Mr. Collins and the other was assigned in the name of his deceased brother who had died in 1943. SSA assigned the latter SSN in 1963, after the brother's death. SSA made RSI payments in the amount of $32,723 between 1993 and 1998 to Mr. Collins in the name of his deceased brother. Mr. Collins admitted to fraudulently obtaining an SSN and title II RSI payments from SSA using his deceased brother's identity. Mr. Collins was employed full-time while collecting these SSA payments and earned substantial wages under his true SSN. It was later determined that Mr. Collins had cashed $28,243 of the SSA checks. The remaining $4,480 had been returned to SSA by the U.S. Postal Service who had been unable to deliver the checks due to a change of address.

Title XVI Disability (SSI) Recipient Commits Identity Theft

On April 13, 2001, Mr. David Melgoza-Solis, a Mexican citizen, was sentenced to 6 months in custody of the Bureau of Prisons and ordered to pay $200 in assessment fees in violation of one count of 42 U.S.C. § 1383a, "Fraudulent acts; penalties; restitution" and one count of 42 U.S.C. § 1542 "Transfer of funds from other Federal agencies to Secretary of Housing and Urban Development." Mr. Melgoza-Solis was also sentenced to supervised release for a term of 3 years and will be subject to an INS Deportation Hearing. SSA waived restitution of the $80,485 fraud loss to the SSI program.

Since 1975, Mr. Melgoza-Solis had been fraudulently using the identity of Mr. Fred Gabes Cruz with a counterfeit New Mexico Certificate of Birth. In February 1989, Mr. Melgoza-Solis applied for and received SSI benefits in the name of Fred Gabes Cruz. SSI benefits continued through December 2000. The total SSI overpayment due to fraudulent identity information is $80,485. Mr. Melgoza-Solis was subsequently arrested and charged with violating 42 U.S.C. § 1542 and 42 U.S.C. § 1383a. On January 16, 2001 Mr. Melgoza-Solis pled guilty to both counts.

5. For the Last Five (5) Fiscal Years, State the Number of SSA Employee Cases that OIG Investigated Where SSA Employees Disclosed, Sold, or Released SSN Information. Also, Describe the Nature and Resulting Criminal or Administrative Action of Each Case.

In the past 5 fiscal years, OIG investigated 55 cases involving 61 employees. In Appendix A of this report, we present, by case and fiscal year, the nature of each allegation, the criminal actions including sentences and restitution ordered, and SSA administrative actions taken. Generally, the allegations involved submission/processing of false SSN applications, selling legitimate SSNs, selling counterfeit SSN cards and general SSN Misuse. A majority of these cases resulted in criminal convictions.

6. Suggest How SSA Can Improve How It Provides Information to the Public on the Proper Use and Dissemination of the SSN.

We believe that public awareness is one of the most effective tools in fighting the crime of identity fraud. To its credit, SSA has attempted to increase public awareness in several different manners, including issuing a publication related to the subject, providing information on the SSA website, holding "town hall" meetings with various entities and working with the Federal Trade Commission in developing information for the public. In addition to these measures, we believe the following suggestions may assist SSA in its efforts to inform the public of the proper use and dissemination of SSNs.

- The SSA website is an excellent tool for educating the public about the proper use of the SSN. Although already being utilized, SSA's OIG and Communications Office could team up to provide additional information. For example, articles could be posted on the site in the form of interesting "Tips" and "Tactics," which would be designed to educate and remind the general public about the potential dangers of sharing one's SSN with non-governmental and suspicious entities.

- SSA could include informational pamphlets when issuing SSN cards and retirement and benefits statements to the public. These pamphlets could remind the public about SSN misuse and provide them with the OIG Fraud Hotline Toll-Free Number.

- Additional "Identity Theft Awareness Workshops" or "Town Hall Meetings," could be instituted in conjunction with organizations whose clients are the elderly and/or the disabled.

- Public Service Announcements such as advertisements on radio, television, and in leading senior citizens and national publications would be helpful in reaching the public-at-large.

- SSA could distribute informational literature to commercial, governmental and non-profit entities that outlines (1) the authorized uses of SSNs and (2) the organizations' responsibilities for protecting this sensitive personal information.

7. Evaluate SSA's Efforts to Work with Other Federal Agencies, Particularly the Internal Revenue Service and the Immigration and Naturalization Service, in Identifying and Preventing SSN Misuse.

We are aware that SSA has worked successfully with certain Federal agencies in its efforts to identify and combat SSN misuse. For example, SSA and SSA's OIG frequently collaborate with the Federal Trade Commission, which is the Federal agency serving as the centralized complaint and consumer education service provider for victims of identity theft. Additionally, SSA, IRS, and INS have had some meaningful cooperative efforts to address this issue.

For example, as a result of an IRS and SSA data match, IRS has begun to notify taxpayers and disallow some exemptions and/or deductions when the name and SSN of an individual listed on a tax return does not match SSA's records. In such cases, an individual who has been the victim of identity theft is alerted to the discrepant information and, if necessary, can begin to take corrective measures.

SSA has also been working with INS and the State Department to implement an "Enumeration at Entry" program for noncitizens who wish, and are eligible, to receive an SSN. With this program, INS will gather necessary information for noncitizens qualified to receive an SSN during the applicants' entry interviews. We are certainly encouraged by this concept. In fact, we believe that, once fully implemented, the program will be an important step in preventing the improper attainment of SSNs by noncitizens who present counterfeit immigration documents at SSA field offices. However, we have some concerns regarding the length of time the implementation of this initiative is taking. Given recent national tragedies, we believe full implementation of the Enumeration at Entry program should be given priority and expedited by the Agencies.

Other efforts that SSA has made to coordinate with IRS and INS have not always been successful. The Agency relies on other Federal agencies to assist in combating SSN misuse. Specifically, as provided by law, SSA must rely on the IRS to enforce penalties for inaccurate wage reporting and the INS to enforce immigration laws. Unfortunately, the IRS has been reluctant to apply penalties and SSA and the INS have had limited and protracted collaboration on the issue.

IRS RELUCTANT TO APPLY PENALTIES

In a previous OIG audit, SSA senior staff stated that employers have no incentive to submit accurate annual wage reports because the IRS rarely enforces existing

penalties.[14] SSA staff believed applying penalties would have a rippling effect on employers who consistently submit wage reports for employees whose names and SSNs do not match SSA's records. Although SSA is primarily only interested in penalizing the most egregious employers, IRS staff expressed concern with the application of even these penalties. IRS senior staff members believe they and SSA would have a difficult time determining whether an employer exercised appropriate diligence in obtaining the necessary information from employees. SSA representatives, however, believe the Agency could provide the IRS with sufficient evidence to show an employer knew or should have known its employees' SSNs were incorrect

Despite the IRS' concerns, the two Agencies held discussions to explore the enforcement of an existing penalty provision ($50 per incorrect wage report) for employers who repeatedly submit erroneous name and/or SSN information. To implement the penalty, SSA and IRS agreed the Agencies must (1) jointly define the circumstances for applying penalties, (2) identify information needed from SSA for the IRS to support applying penalties, and (3) develop the proposed data flow and procedures to be followed.

In Calendar Year 2000, SSA provided a list of 100 of the most egregious employers to the IRS. These employers represented those with the largest number of name/SSN match failures in consecutive years. IRS expressed interest in the listing but, to date, has not assessed penalties.

LIMITED COLLABORATION BETWEEN SSA AND THE INS TO ADDRESS GROWTH OF ESF

During a previous audit, both SSA and INS senior staff told us collaboration between the two Agencies has been limited.[15] In SSA's December 1997 version of its *ESF Tactical Plan*, the Agency included an initiative to develop a better understanding of the extent that immigration issues may contribute to name and SSN mismatches and the ESF's growth. The initiative was to involve SSA working with the INS to formulate and conduct a limited review of employers who (1) employ large number of immigrants and (2) experience high name and SSN error rates in their annual wage reporting. According to SSA representatives, because of privacy and disclosure limitations, the Agency determined it could not share such information with the INS. Therefore, SSA did not include this project in subsequent versions of the *ESF Tactical Plan*.

[14] SSA/OIG report entitled *Obstacles to Reducing Social Security Number Misuse in the Agriculture Industry*, January 2001 (A-08-99-41004).

[15] SSA/OIG report entitled *Obstacles to Reducing Social Security Number Misuse in the Agriculture Industry*, January 2001 (A-08-99-41004).

8. Recommend Methods to Improve SSA's Processes And Procedures to Prevent Future SSN Misuse.

In addition to the items discussed in response to previous questions, we also believe SSA should expand its data matching activities with other Federal, State, and local government entities and explore other innovative technologies such as biometrics. Data matching also known as computer matching, has three main goals: (1) to determine eligibility for Federal benefits; (2) to determine compliance with Federal benefit program requirements; and (3) to effectuate recovery of improper payment or delinquent debts from current or former beneficiaries of Federal benefits.

The *Computer Matching and Privacy Protection Act of 1988* (CMPPA), (Public Law 100-503) requires Federal agencies to enter into written agreements with other agencies or non-Federal entities before disclosing records for use in computer matching programs. The law also specifies areas to be addressed in such agreements, including justification for matching, notifying individuals (including Federal employees) whose records are to be matched, procedures for retention and destruction of data after matching, and prohibitions on disclosure of records and the compilation of data. CMPPA also requires that a copy of each agreement be transmitted to specified congressional committees and be available to the public upon request.

SSA has a number of matching agreements in place to share information with State agencies. For example, SSA has agreements with Bureaus of Vital Statistics to identify unreported marriages and divorces for title II and XVI beneficiaries. Based on recent audit results, SSA could benefit from expanding computer matches with States and other Federal agencies to include individuals who had benefits terminated due to confirmed or suspected fraud.[16]

Biometrics is the science of measuring unique physical characteristics, such as fingerprints, for purposes of identification. As such, Biometric technologies offers a potentially foolproof means of verifying an individual's identity and, if used during the enumeration and benefit application processes, can detect and prevent applicants' attempts to improperly obtain benefits and services. This technology is particularly important, given the expanded use of the SSN as a national identifier.

Our previous audit work indicates that 11 States have implemented or planned to adopt Biometric technologies in their social service programs.[17] As a result of these programs, States have reported significant monetary savings. Based on this audit work, we believe SSA could benefit from pursuing matching agreements with these States to identify individuals who also may be inappropriately receiving SSA benefit payments.

---

[16] SSA/OIG report *The Social Security Administration is Pursuing Matching Agreements with New York and Other States Using Biometric Technologies*, January 2000 (A-08-98-41007).

[17] SSA/OIG report *The Social Security Administration is Pursuing Matching Agreements with New York and Other States Using Biometric Technologies*, January 2000 (A-08-98-41007).

While the use of Biometrics may present privacy concerns, given the tragic events that have recently affected our Nation's security, we must seriously weigh these concerns against the need for protecting our critical assets. Similarly, SSA has a duty to Congress and the American public to balance such concerns with its role to ensure the integrity of the SSN and its programs.

9. Please Provide the Current Data Matching Initiatives SSA has Underway to Detect and/or Prevent SSA Overpayments to Individuals the Agency Determines are Residing in Nursing Homes and Prisons. Also, Comment on the Effectiveness of these Data Matches and Describe any Further Initiatives that Might Improve this Process. Further, Itemize for the Last Five (5) Years the Amount of SSA Overpayments Made to Individuals in Nursing Homes and Prisons because SSA was Unaware that Their Care was Paid by Medicare. Please Itemize the Amounts by Year.

SSA has a number of data matching initiatives underway to detect and/or prevent overpayments to individuals residing in nursing homes and prisons. Specifically, SSA matches its payment records with nursing home data from the Centers for Medicare and Medicaid Services (CMS),[18] as well as with Federal, State, and local prisons. Specific initiatives are described below.

NURSING HOMES

In December 1998, SSA initiated a computer match with CMS to detect instances in which SSI recipients, institutionalized in nursing homes, were being overpaid.[19] This match, which covers all the States, was also conducted in March 1999 and again in September 1999. Then in FY 2000, the match was performed on a monthly basis and it continues to be performed today.

In October 2000, SSA's Office of Quality Assurance and Performance Assessment (OQA) issued a report on its assessment of SSA's match with nursing home data. OQA found that in FY 1999, the data match between SSA and CMS identified overpayment benefits of $27 million that could have been either recovered or prevented at a cost of $6.8 million.

OQA also found that nursing home data received from CMS was not sufficiently accurate for SSA to institute automatic payment changes. Specifically, some of CMS' data fields (such as length of stay and source of payment) contained missing or inaccurate data. As such, OQA concluded that CMS needs to improve the reliability of

[18] CMS was formerly known as the Health Care Financing Administration (HCFA).

[19] Prior to 1998, SSA matched its payment records with HCFA nursing home data. However, the HCFA data was limited since it did not contain all the States. SSA estimated program savings from this limited match of $3.8 million per year.

its data before SSA could use it to suspend payments without verification. In FY 2002, OQA is scheduled to conduct a follow-up review to determine the accuracy of the CMS data and the approximate time for SSA field offices to process a case resulting from the data match.

OIG does not have a tracking system in place to capture the amount of SSI overpayments resulting from individuals living in nursing homes. Therefore, we are unable to provide statistics for the past 5 years, and hence defer this question to SSA.

PRISONERS

SSA receives prisoner data from approximately 5,500 Federal, State, county, and local correctional agencies. This data, which accounts for over 99 percent of the prisoner population in the United States, is matched against SSA payment records in order to identify, prevent and/or recover overpayments to prisoners. If the data matching identifies benefit payments paid to a prisoner, the appropriate SSA office is notified and staff verify the person's identity and determine whether payments should be stopped. Once payments cease, any overpayment amounts are computed and an account is established on the individual's record to control the return of amounts overpaid.

SSA's Chief Actuary estimated a cost avoidance of $125 million to be realized semiannually from 1995 to 2001. Since the OIG does not have a system in place to track overpayments to prisoners, we defer to SSA to provide statistics for the past 5 years.

In 1996 and 1997, the OIG completed two audits pertaining to SSA's prisoner matching operations.[20] Specifically, we reported the following.

- SSA was only achieving limited success in obtaining prisoner information and using it to prohibit benefit payments. Specifically, we estimated overpayments to prisoners in Federal, State, and county or local correctional facilities in the amount of $48.8 million. These overpayments were due to the delays in receiving information from correctional facilities. Our report included recommendations to: (1) make current procedures for obtaining prisoner information more effective; (2) explore alternatives to the current system in place for obtaining prisoner information; and (3) make the administrative processes associated with prisoner information more effective.

- SSA was not always detecting and stopping benefit payments to prisoners due to control weaknesses in its prisoner record matching program and in its prisoner alert procedures. Also, we found that SSA had limited success in attempting to recover overpayments made to prisoners. Our report included recommendations for: (1) improving the matching procedures for identifying prisoners receiving benefits;

[20] SSA/OIG reports entitled *Effectiveness in Obtaining Records to Identify Prisoners*, May 1996 (A-01-94-02004) and *Effectiveness of the Social Security Administration's Procedures to Process Prisoner Information, Suspend Payments and Collect Overpayments*, June 1997 (A-01-96-61083).

(2) processing prisoner alerts more effectively; and (3) improving the collection of overpayments from prisoners.

In FY 2002, we are initiating a follow-up review to our 1996 and 1997 audit reports. We will assess SSA's efforts to implement the recommendations made in these two reports and identify any further areas for improving prisoner data matching operations. Based on preliminary work started in FY 2001, SSA has made great strides in improving the detection and prevention of overpayments to prisoners since our work in 1996 and 1997. Once our follow-up work is completed in FY 2002/2003, we will comment in detail on the effectiveness of SSA's prisoner operations to prevent overpayments and possible initiatives, if necessary, for further improvement.

Conclusion

We recognize that the issue of SSN misuse is complex and impacts many public and private programs. With the Internet as a catalyst, SSN misuse and identity fraud have soared to new heights, partially as a result of the ease in which individuals can access personal information and false documents on-line. To its credit, SSA has made strides in improving systems and processes in the fight against these abuses. However, we believe more needs to be done. We understand the need to provide timely, world class customer service, but it is important to strike a balance between expediency and stewardship responsibilities.

Recently, we provided the Acting Commissioner of Social Security with a list of prior audit recommendations that the Agency either disagreed with or had not yet implemented. In light of recent events, the Acting Commissioner planned to review these recommendations to determine whether any should be reconsidered and/or expedited. We are encouraged by this action and hope SSA will reconsider recommendations reiterated in this report that will serve to improve the integrity of the SSN.

Appendices

Scope and Methodology

Much of our work was based on published reports from the past 2 years. We performed report review work in Birmingham, Alabama. Analytical work on matching initiatives and overpayments was performed in Boston, Massachusetts. Also, other work, including interviews and observations regarding undeliverable SSNs and gathering of investigative case data was performed at SSA Headquarters in Baltimore, Maryland. We completed our field work between August 2001 and September 2001.

EMPLOYEE CASE STATISTICS FOR PAST FIVE FISCAL YEARS

Fiscal Year 1997

Nature of Allegations	Criminal Action	Sentencings	Restitution Ordered	Administrative Actions
False Application				Termination
Selling SSNs	PTD			Termination
Selling SSNs	Conviction	04/29/97 6 months Incarceration, 2 years & 6 months Probation		Termination
Selling SSNs	Plea	05/02/97 3 years Probation		Termination
Selling SSNs	Plea	07/03/97 3 years Probation	$20,239 (NONSSA)	Termination
Selling SSNs	Conviction	04/30/97 2 years Probation		Suspension
SSN Misuse				Suspension

SSN = Social Security Number
PTD = Pre-Trial Diversion

Fiscal Year 1998

Nature of Allegations	Criminal Action	Sentencings	Restitution Ordered	Administrative Actions
False Application/ SSN Card	Conviction	07/01/1998 1 year 3 months Incarceration, 2 years Probation		Retired
False Application/ SSN Card	Conviction	04/14/1999 2 years Probation		Resigned
Selling SSNs	Conviction	06/24/1998 1 year, 1 day Probation	$306,727 (NONSSA)	Resigned
SSN Misuse				Resigned
Selling SSNs	Conviction	08/04/1997 3 years Probation		Termination
Selling SSNs	Conviction	07/14/1997 10 months. Incarceration, 2 years Probation	$10,000 (NONSSA)	Termination
SSN Misuse	Conviction	02/09/1998 3 years 2 months Incarceration		Termination
Selling SSNs	Conviction	09/17/1998 1 year Incarceration, 3 years Probation	$138,186 (NONSSA)	Termination
SSN Misuse	Conviction	05/18/1998 1 year Probation		Resigned
SSN Misuse				Termination
Selling SSNs	Conviction	03/10/1998 5 years Probation		Resigned
SSN Misuse	Conviction	07/29/1998 4 months Incarceration, 4 years Probation		Resigned
SSN Misuse	Convictions (two employees)	02/25/1998 5 years Probation	$174,312 $20,993	Termination

Fiscal Year 1999

Nature of Allegations	Criminal Action	Sentencings	Restitution Ordered	Administrative Actions
False Application/ SSN Card	Conviction	12/18/1998 6 months. Incarceration, 3 years Probation	$8,158 (NONSSA)	Termination
False Application/ SSN Card	Conviction	02/16/1999 5 years Probation		Resigned
SSN Misuse	Convicted 6 employees	03/14/1997 4 years Probation 07/10/1997 3 years Probation 04/16/1998 5 years Probation 02/22/1999 1 year Probation 03/03/1999 2 years Probation 06/16/1999 6 months Incarceration, 2 years Probation		Resigned Suspension Resigned Resigned Suspension Suspension
SSN Misuse				Resigned
SSN Misuse	Conviction	02/28/1998 2 years Probation		Termination
SSN Misuse	Conviction	06/30/1998 3 years Probation	$264,781 (NONSSA)	Termination
SSN Misuse	Conviction	02/10/1999 6 months Incarceration, 2 years Probation		Termination

Fiscal Year 2000

Nature of Allegations	Criminal Action	Sentencings	Restitution Ordered	Administrative Actions
SSN Misuse	Conviction	10/27/1999 2 years Probation		Resigned
Selling SSNs	Conviction	01/27/2000 1 year Incarceration, 3 years Probation	$64,582 SSA	Resigned
SSN Misuse	Conviction	12/01/1999 3 years Probation		Leave Without Pay
SSN Misuse				Resigned
Selling SSNs	Conviction	07/28/2000 7 months Incarceration, 2 years Probation		Termination
Selling SSNs	Conviction	03/06/2000 4 months Home detention, 3 years Probation		Resigned
Selling SSNs	Conviction	03/27/2000 6 months Home detention, 3 years Probation		Resigned
Selling SSNs	Conviction	03/06/2000 2 months Incarceration, 3 years Probation	$545,000 (NONSSA)	Resigned
Selling SSNs	Conviction	02/14/2000 14 months Incarceration, 3 years Probation	$32,577 (NONSSA)	Resigned
Selling SSNs				Resigned
SSN Misuse	Conviction	04/20/2000 3 years Probation		Termination
SSN Misuse	Illegal Alien			Resigned
SSN Misuse	Conviction	03/06/2000 4 months Incarceration, 4 months Home detention, 3 years Probation		Termination
Misuse Computer	Conviction	01/28/2000 6 months Incarceration, 3 years Probation		Resigned
SSN Misuse				Resigned
Misuse Computer	Conviction	02/08/2000 3 years Probation	$200,000 (NONSSA)	Resigned

Fiscal Year 2001

Nature of Allegations	Criminal Action	Sentencings	Restitution Ordered	Administrative Actions
SSN Fraud	Conviction	05/09/2001 12 months Home confinement, 5 years Probation	$10,000 (NONSSA)	Resigned
False Application	Conviction	12/21/2000 6 months Incarceration, 2 years Probation		Termination
Selling SSNs				Resigned
False Application	Conviction	9/15/2000 6 months Incarceration, 3 years Probation	$435,895 (NONSSA)	Resigned
Selling SSNs				Resigned
SSN Misuse	Conviction	03/30/2001 27 months Incarceration, 3 years Probation		Resigned
Counterfeit SSN	Plea	06/08/2001 6 months. Incarceration, 2 years probation	$52,718 (NONSSA)	Retired
SSN Fraud	Conviction	01/17/2001 15 months Incarceration, 36 months Probation		Resigned
SSN Fraud	Conviction	10/31/2000 6 months Incarceration, 3 years Probation	$350,000 (NONSSA)	Resigned
SSN Fraud	Conviction	05/01/2001 18 months Incarceration		Resigned
SSN Misuse	PTD			Suspension
Identity Theft	Conviction	07/27/2001 3 years Probation		Resigned

Appendix C

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kim Byrd, Acting Director, Operations Audit Division (205) 801-1605

Acknowledgments

In addition to those named above:

Kathy Youngblood, Senior Auditor

Walter Bayer, Deputy Director

Judith Oliviera, Senior Auditor

Katie Hallock, Auditor

Tom Sipes, Special Agent-in-Charge

Tim DeHoff, Investigator

For additional copies of this report, please visit our web site at http://www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 966-1375. Refer to Common Identification Number A-08-02-22030.