

Office of the Inspector General

May 28, 1999

Kenneth S. Apfel
Commissioner of Social Security

Acting Inspector General

Management Advisory Report: Using Social Security Numbers to Commit Fraud

The attached final management advisory report is to inform the Social Security Administration's (SSA) management about the use of Social Security numbers (SSN) to commit fraud (A-08-99-42002). The objective of this report is to inform SSA officials of certain trends identified during the Office of the Inspector General's audit and investigative work involving the fraudulent use of SSNs. Also, we present specific recommendations that we believe SSA should consider which track well with the Agency's "Zero Tolerance for Fraud" initiatives.

You may wish to comment on any further action taken or contemplated on our recommendations. If you choose to offer comments, please provide them within the next 60 days. If you wish to discuss the final report, please call me or have your staff contact Daniel R. Devlin, Acting Assistant Inspector General for Audit, at (410) 965-9700.

James G. Huse, Jr.

Attachment

**OFFICE OF
THE INSPECTOR GENERAL**

SOCIAL SECURITY ADMINISTRATION

**USING SOCIAL SECURITY
NUMBERS TO
COMMIT FRAUD**

May 1999 A-08-99-42002

**MANAGEMENT
ADVISORY REPORT**



EXECUTIVE SUMMARY

The objective of this management advisory report is to inform Social Security Administration (SSA) officials of certain trends identified during the Office of the Inspector General's (OIG) current audit and investigative work involving the fraudulent use of Social Security numbers (SSN). Also, we will present specific recommendations that we believe SSA should consider to buttress the Agency's "Zero Tolerance for Fraud" initiative. The issue of identity fraud is a rising national concern. In response, Congress enacted the *Identity Theft and Assumption Deterrence Act of 1998*, which made identity theft a Federal crime, punishable by substantial penalties.

During our audits and investigations, we have identified cases in which SSNs were obtained using fraudulent documentation. Once obtained, these SSNs were often used to commit identity fraud. We currently have an audit underway entitled, *Review of SSA's Procedures for Verifying Evidentiary Documents Submitted with Original SSN Applications* (CIN: A-08-98-41009), in which we are examining SSA's enumeration policies and procedures. We will issue a separate report to address specific findings resulting from the audit once the assignment has been completed. However, we believe that some of the preliminary results related to SSN fraud warrant the immediate attention of SSA management.

The issue of identity fraud is a new and emerging area. In the past, resources have not been devoted to this issue because our staff worked in areas that provided a visible cost benefit to SSA and the trust funds. Since SSA became an independent Agency in 1995, the SSA Fraud Hotline has recorded a steady increase in SSN misuse allegations. Although we acknowledge that much of this growth can be attributed to an increase in staff available to answer and respond to Hotline calls, we believe this trend is also related to the emergence of identity fraud. Additionally, OIG audits and investigations have clearly identified that the integrity of the Agency's enumeration process materially impacts on fraud, waste, and abuse at SSA.

RESULTS OF REVIEW

Congress and other Federal agencies have noted that the SSN is an integral part of the identity fraud crime. The importance placed on SSNs in today's society provides a tempting motive for many unscrupulous individuals to fraudulently acquire a SSN and use it for illegal purposes. For example, one individual and his associates obtained 1,120 SSNs for nonexistent children using fraudulent birth certificates. Some of the "identities" acquired through this scheme were used to defraud credit card companies of approximately \$30 million. Additionally, during an ongoing audit, we identified 1,447 addresses at which almost 33,000 SSNs were sent during a 7-month period (an

average of almost 23 cards to each address). Our preliminary analysis of 3,500 SSNs that were sent to 90 of these addresses has disclosed numerous cases in which SSNs were obtained using fraudulent documentation.

Occurrences of identity fraud that were investigated by the U.S. Secret Service resulted in losses by victimized individuals and institutions of approximately \$745 million in Fiscal Year (FY) 1997. This figure increased from \$442 million in FY 1995. We recognize that the responsibility for controlling this trend cannot and should not fall solely on SSA. Nevertheless, we believe that the Agency needs to evaluate whether it can do more to ensure the security and integrity of its enumeration function. SSA has a difficult balancing act to perform in providing “World-Class Service” and enforcing its “Zero Tolerance for Fraud” goals. However, in light of the proliferation of SSN fraud cases and the concerns of both Congress and the American public, we believe that SSA should consider the implementation of more security measures, recognizing that these steps may impact customer service. We are aware that impacting customer service with increased security measures represents a difficult choice for SSA; however, in our view, the proliferation of identity fraud crimes warrants this approach.

Our report includes descriptions of selected SSN fraud cases, which OIG investigated and subsequently referred to the Department of Justice for prosecution. Additionally, we have included observations noted during other audits and investigations regarding the use of SSNs to commit identity fraud. We believe these cases provide an exceptional learning opportunity for SSA and should serve as a catalyst for changes essential to ensuring the integrity of the Agency’s enumeration responsibility.

CONCLUSIONS AND RECOMMENDATIONS

We believe that SSA must make both philosophical and procedural changes to ensure the integrity of its enumeration function. Most importantly, we believe that SSA should make it clear through its policies and performance measures that fraud prevention measures should never be circumvented to satisfy customer service demands. Further, we recommend that SSA:

- Incorporate preventive controls in its Modernized Enumeration System (MES) that address certain disturbing circumstances noted in our investigations.
- Require verification from the issuing State when an out-of-State birth certificate is presented as evidence for a SSN application.
- Continue its efforts to have the Immigration and Naturalization Service (INS) and the State Department collect and verify enumeration information for aliens. However, if an alien chooses to visit a SSA field office (FO) to apply for his or her SSN, require the SSA FO to obtain independent verification of the alien’s documentation before approving the SSN application.

AGENCY COMMENTS

In its response, SSA recognized that the public's confidence in its stewardship of Agency programs is undermined when individuals succeed in abusing Agency systems. Additionally, the Agency acknowledged that instances of identity and noncitizen fraud have a significant societal impact. To address specific recommendations outlined in our report, SSA detailed numerous ongoing and future initiatives that it believed would correct identified weaknesses and reduce the possibility that similar cases of fraudulent SSN attainment will recur.

As stated in our first recommendation, the Agency plans to issue a reminder to FO personnel regarding the importance of adhering to fraud prevention procedures, irrespective of customer service demands. Additionally, SSA plans to review current public relations vehicles and explore opportunities to reemphasize to the public the importance of fraud prevention activities.

In responding to our second recommendation that SSA incorporate certain preventative controls in MES, the Agency cited three initiatives. SSA referred to provisions of the Taxpayer Relief Act of 1997, which the Agency believes will deter individuals from obtaining SSNs for nonexistent children. SSA stated that it will work with the OIG to target potential fraudulent activity when multiple SSNs are sent to the same address. Finally, SSA recently began using a new version of one integrity software program that, among other features, "alerts" the applicable FO any time four or more SSN cards are sent to the same address in a 5-week period.

In response to our third recommendation concerning independent verification of out-of-State birth certificates presented as evidence for SSN applications, SSA asserted that this action would be impractical for the public and SSA FOs. Instead, the Agency stated that it hoped to obtain on-line access to State vital records data at sometime in the future.

To address recommendation four, SSA plans to continue its efforts to have INS and the State Department collect enumeration information for noncitizens. In response to recommendation five, that SSA require independent verification of alien evidentiary documents when noncitizens apply for SSNs at FOs, the Agency stated that it would continue to be vigilant to guard against fraudulent documents and would work with INS in attempting to shorten the verification process.

SSA also provided technical comments that were considered and incorporated, where appropriate, in this final report. The full text of SSA's comments is included in Appendix A.

OIG RESPONSE

We acknowledge the steps SSA has taken and contemplated in attempting to combat SSN fraud and believe that the Agency's response and planned actions adequately

address two of our recommendations (recommendations 1 and 4). Nevertheless, we believe the ongoing or planned initiatives SSA cited to address the remaining three recommendations (recommendations 2, 3, and 5) do not effectively respond to our goal of **preventing** the fraudulent attainment of SSNs.

Although the initiatives SSA described in response to our recommendation that SSA implement preventive controls in MES (recommendation 2) have merit, they appear to 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. Therefore, we believe that SSA must hold itself accountable for preventing SSNs from being obtained through fraudulent means. As suggested in our recommendation, we believe the Agency's initiatives should focus on front-end controls within MES that will preclude the issuance of SSNs in certain defined circumstances.

In response to our recommendation that FOs obtain independent verification of out-of-State birth certificates (recommendation 3), SSA described an initiative that is contemplated for future years. Specifically, SSA hopes to gain on-line access to State vital records data so that FOs can verify birth and death records provided by SSA customers. The implementation of this initiative is contingent on obtaining agreements with all of the States and jurisdictions—first for accessing in-State data and then separate agreements so that data can be shared across State lines. While this goal will certainly prove worthy in the future, implementation may be years away. In the meantime, we believe SSA should reconsider our recommendation to independently verify out-of-State birth certificates. Given the reduction in newborn SSN applications processed by FOs as a result of the enumeration-at-birth process and the infrequency that out-of-State birth certificates are presented with SSN applications, we do not believe that this requirement would be impractical.

Finally, in its response, SSA stated that it planned to be vigilant in its efforts to guard against the submission of fraudulent documents by aliens applying for SSNs at FOs. However, the Agency did not agree to require independent verification of alien documents (recommendation 5). We do not support SSA's approach. As evidenced by the cases presented in this report, current SSA procedures have not always been successful in preventing the attainment of SSNs with fraudulent alien documents. We acknowledge SSA's efforts in working with INS to improve and shorten the verification process (e.g., the time lag in INS' Systematic Alien Verification for Entitlements system.) However, we have held our own conversations with INS personnel and believe that the INS system improvements necessary to effect positive changes within SSA's verification process will take years to implement. Again, we believe it is imperative that SSA institute controls to **prevent** the issuance of SSNs based on fraudulent documents. By doing so, the Agency can ensure that it is doing its part to control the growing identity fraud trend. Until such time that alien documents are independently verified by the issuing agencies, we do not believe that SSA can accomplish this goal. Accordingly, we encourage SSA to reconsider our recommendation.

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	i
INTRODUCTION	1
RESULTS OF REVIEW	6
FRAUDULENT BIRTH CERTIFICATES USED TO OBTAIN 1,120 SSNS.....	6
COUNTERFEIT ALIEN DOCUMENTS USED TO OBTAIN SSNS.....	8
▪ Limitations in INS' SAVE Program	9
▪ Limitations of the SSA/INS/State Department Memoranda of Understanding.....	9
▪ Example of Counterfeit INS and Polish Documents Used to Obtain Over 250 SSNs	10
▪ Ongoing Audit Uncovered Numerous Potential Cases in Involving Fraudulent INS Documents Used to Obtain SSNs	11
IMPACT OF SSN FRAUD ON SSA PROGRAMS	13
▪ Conflict Between SSA's Strategic Goals	13
▪ Benefits Paid Inappropriately	14
▪ Suspense File Postings.....	14
▪ SSA Resources Currently Required to Address SSN Fraud	15
IMPACT OF IDENTITY FRAUD ON INDIVIDUALS AND ENTITIES EXTERNAL TO SSA.....	15
CONCLUSIONS AND RECOMMENDATIONS	17
AGENCY COMMENTS AND OIG RESPONSE	17
 APPENDICES	
APPENDIX A - SSA Comments	
APPENDIX B - Major Report Contributors	
APPENDIX C - SSA Organizational Chart	

INTRODUCTION

OBJECTIVE

The objective of this management advisory report is to inform Social Security Administration (SSA) officials of certain trends identified during the Office of the Inspector General's (OIG) current audit and investigative work involving the fraudulent use of Social Security numbers (SSN). Also, we will present specific recommendations that we believe SSA should consider to buttress the Agency's "Zero Tolerance for Fraud" initiative.

BACKGROUND

One of the key elements SSA employs to accurately and efficiently administer the Nation's Social Security system is the SSN. As mandated in 1935 by title II of the Social Security Act, SSA must maintain records of wage amounts that employers pay to individuals. To facilitate this responsibility, in 1936 SSA created SSNs as a method of maintaining individual earnings records and issued workers cards as a record of their SSN. SSA refers to the process of assigning SSNs to U.S. workers and Social Security beneficiaries as enumeration.¹

Fraudulent Uses of SSNs

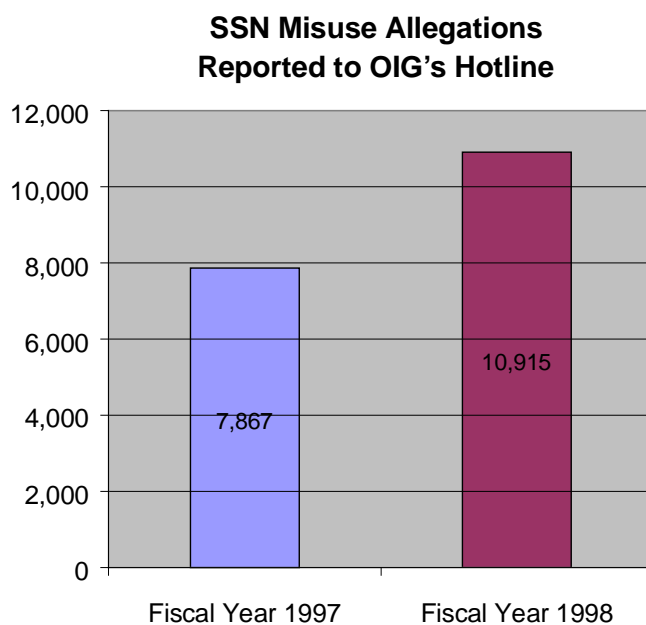
SSA statistics show that approximately 277 million individuals currently have SSNs. The magnitude of the enumeration area and the importance placed on SSNs in today's society provides a tempting motive for many unscrupulous individuals to fraudulently acquire a SSN and use it for illegal purposes. Almost every day, national and local news organizations report on crimes that are committed using stolen or fraudulent SSNs. These crimes not only affect the Government's ability to administer programs, but also impact individual citizens' attempts to receive and maintain satisfactory credit standings, as well as obtain other Government and private benefits.

The fraudulent attainment and use of SSNs can be generally categorized as identity fraud, or the illegal use of personal identifying information to commit financial fraud. Identity fraud can encompass a host of crimes, ranging from the unauthorized use of a credit card to a comprehensive takeover of another person's identity and financial accounts. We have classified the types of identity fraud in the following three categories.

¹ The enumeration area also includes the issuance of replacement cards to people with existing numbers and verification of SSNs for employers and other Government agencies.

- **Identity Theft** – Misusing a third party’s SSN to obtain credit in that person’s name.
- **New SSN Fraud** – Acquiring a new SSN to improperly: 1) obtain Government benefits, such as welfare benefits, food stamps, education loans, Veteran’s benefits, Small Business Administration loans, Medicaid, worker’s compensation, Temporary Assistance to Needy Families; 2) conceal bad credit; or 3) avoid arrest warrants.
- **Alien Fraud** – Misusing a third party’s SSN or obtaining either a SSN using fraudulent documentation or a counterfeit SSN card for work purposes.

SSA became an independent agency in April 1995. In 1996, SSA’s OIG created a Hotline that employees and the public can contact with allegations of fraud, waste, or abuse related to the Agency. Since the implementation of this Hotline, OIG has noted a significant increase in the number of allegations made regarding SSN fraud. Although we acknowledge that much of this growth can be attributed to an increase in staff available to answer and respond to Hotline calls, we believe this trend is also related to growth of the identity fraud issue. As shown in the chart below, the SSA Fraud Hotline received 7,867 allegations that were related to SSN fraud in Fiscal Year (FY) 1997. In FY 1998, the Hotline received 10,915 allegations that were SSN-related. Based on allegations received during the first quarter of the current FY, we anticipate a significant increase of SSN-related allegations during this year.



Congressional Response to Identity Fraud

As a result of the increasing incidences of identity fraud using SSNs, SSA, Congress, and the American public have become acutely aware of the need for SSA to exert tight

control over the enumeration process. In recent years, Congress has mandated several studies related to this area.² SSA management and officials from other Federal agencies have also testified before Congress regarding fraud detection and prevention.³

In October 1998, Congress enacted the *Identity Theft and Assumption Deterrence Act of 1998* (Act). The Act provides SSA with additional weapons to fight identity fraud and strengthens existing authorities under the criminal code. In general, the Act made identity theft a Federal crime, punishable by substantial penalties. The Act included the following provisions:

- Expanded the previous definition of identity theft included in Federal Law. Specifically, the prior definition primarily addressed the use or transfer of identity documents (e.g., Social Security card, birth certificate). However, the new Act addresses the theft or use of a person's identifying information (e.g., SSN, date of birth, mother's maiden name).
- Provided for various terms of imprisonment depending upon the facts of the identity theft offense.
- Established the Federal Trade Commission (FTC) as the centralized complaint and consumer education service provider for victims of identity theft. The FTC will provide informational materials to these individuals and refer their complaints to the three major national consumer-reporting agencies and the appropriate law enforcement agencies.

SSA Actions to Address Fraud

Among its recent strategic goals, SSA has addressed the issue of fraud. Specifically, in its Strategic Plan, SSA included the goal "To make SSA program management the best in the business, with **Zero Tolerance for Fraud and Abuse.**" (Emphasis added.) SSA further defines this goal in its *Accountability Report for Fiscal Year 1998* by stating as follows:

"We are setting our standards very high to reflect our view that the public deserves the highest possible level of performance consistent with fiscal

² These studies are summarized in the following reports: SSA's *Report to Congress on Options for Enhancing the Social Security Card*, issued in September 1997; U.S. General Accounting Office's (GAO) report entitled, *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited*, issued May 1998; and the Board of Governors of the Federal Reserve System's *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud*, issued in March 1997.

³ SSA's Associate Commissioner for Policy and Planning testified before the Subcommittee on Immigration and Claims, House Committee on the Judiciary on May 13, 1997 regarding H.R. 231, Secure SSN Card. Federal Trade Commission representatives testified on March 26, 1998, on Internet Privacy before the Subcommittee on Courts and Intellectual Property, House Committee on the Judiciary and on May 20, 1998, regarding the employment eligibility verification process before the Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary.

responsibility. Our assertion of zero tolerance for fraud and abuse means that we will increase our attention on deterring fraudulent activities and on bringing to justice those who practice them”

SSA established the National Anti-Fraud Committee, co-chaired by OIG and comprised of SSA’s executive leadership, to oversee the implementation and coordination of SSA’s strategies to eliminate fraud. The national committee is supported by 10 regional committees, comprised of SSA and OIG staff, which have the primary duty to oversee local policies and strategies. Additionally, SSA implemented several initiatives designed to address the fraudulent attainment and use of SSNs. For example, SSA conducted a study and issued the *Report to Congress on Options for Enhancing the Social Security Card* in September 1997. This study examined several alternatives for issuing counterfeit-resistant SSN cards. Some of the Agency’s other current and planned initiatives include the following.

- *Age 18 and Over Procedures*: SSA implemented unique procedures for processing original SSN applications submitted by individuals age 18 years or older. The purpose of these procedures is to ensure that the applicants do not already have a SSN and are not attempting to inappropriately secure a new SSN.
- *Enumeration Verification System (EVS)*: The EVS provides a mechanism for employers to match employee names and SSNs with SSA’s records. By doing so, employers can ensure that employees have provided accurate information.
- *Access to Systematic Alien Verification for Entitlements (SAVE) Program*: In January 1997, SSA obtained access to the Immigration and Naturalization Service (INS) SAVE program for all of the Agency’s field offices (FO). The SAVE program provides a method for SSA personnel to verify certain INS documents presented as evidence of lawful immigration status or work authority.
- *Collection of Enumeration Data by INS and the State Department*: SSA, INS, and the State Department are currently working on agreements that will enable the latter agencies to collect enumeration data from aliens entering the United States. Although SSA will still process the SSN applications, the agencies believe that this initiative will significantly reduce the possibility of SSA accepting counterfeit documentation and will eliminate duplicate contacts that aliens now must make in order to obtain SSNs.

METHODOLOGY

During the course of an OIG audit⁴, we identified numerous cases in which SSNs may have been obtained using fraudulent documents. Because our OIG investigations have determined that fraudulently obtained SSNs are frequently used to commit identity

⁴ Review of the Social Security Administration’s Procedures for Verifying Evidentiary Documentation Submitted with Original Social Security Number Applications (A-08-98-41009).

fraud, the OIG Offices of Audit and Investigations initiated a joint effort to report this trend to SSA management. As part of this effort, we

- Obtained information from external entities, such as the U.S. Secret Service, the General Accounting Office (GAO), and major U.S. credit card companies;
- Compiled related information from prior OIG reports, current and on-going audits or investigations;
- Obtained SSN-misuse statistics from the SSA Fraud Hotline;
- Analyzed SSA data related to the issuance of SSNs; and
- Interviewed SSA employees to assess the impact of identity fraud and the environment existing within SSA's culture as it relates to this issue.

RESULTS OF REVIEW

Occurrences of identity fraud that were investigated by the U.S. Secret Service resulted in financial losses by victimized individuals and banking institutions of approximately \$745 million in FY 1997. This figure increased from \$442 million in FY 1995. We recognize that the responsibility for controlling this trend cannot and should not fall solely on SSA. Nevertheless, we believe that the Agency needs to evaluate whether it can do more to ensure the security and integrity of its enumeration function. SSA has a difficult balancing act to perform in providing “World-Class Service” and enforcing its “Zero Tolerance for Fraud” goals. However, in light of the proliferation of SSN fraud cases and the concerns and expectations of both Congress and the American public, we believe that SSA should consider the implementation of more security measures. We recognize that these steps may impact some customer performance measures; however, in our view, the proliferation of identity fraud crimes warrants this approach.

The following sections include descriptions of selected SSN fraud cases, which OIG investigated and subsequently referred to the Department of Justice (DoJ) for prosecution. Additionally, we have included observations noted during other audits and investigations regarding the use of SSNs to commit fraud. These cases and observations provide examples of weaknesses in SSA systems and processes that have resulted in the fraudulent attainment of SSNs.

At the completion of its ongoing audit, OIG will report recommendations designed to specifically improve SSA’s operations. However, some of the issues were so important that we believed they needed to be brought to the immediate attention of SSA management. For those items, we are including recommendations in this management advisory report.

FRAUDULENT BIRTH CERTIFICATES USED TO OBTAIN 1,120 SSNS

One of the most egregious cases of SSN fraud uncovered to date involved an individual and his associates who successfully obtained 1,120 original SSNs for nonexistent children. The fraudulent attainment of these SSNs occurred between January 1993 and August 1997 at SSA offices throughout the State of California. To perpetrate the crime, the individual and several other accomplices presented counterfeit Arkansas birth certificates and hospital immunization cards as evidentiary documentation with the applicable SSN applications. Through our analysis of this case, we also noted the following circumstances.

- To facilitate this crime, the individual and several other suspects posed as fathers of the nonexistent children. Although in total they used 15 different aliases, 3 names

were used as the fathers of 994 children. SSA's Modernized Enumeration System (MES) currently has no controls in place that can detect, prior to issuance, when a parent claims to have an unreasonably large number of children.

- The individual and his associates used 36 different addresses to receive the 1,120 SSN cards. However, at 2 of these addresses, the individuals received almost 700 SSN cards. At the remaining 34 addresses, they received between 1 and 194 SSN cards over the 4 ½ - year period. Again, SSA's MES has no controls in place that can detect, prior to issuance, when multiple SSNs have been sent to the same address.
- In February 1994, the California Regional Office issued a fraud alert to its FOs regarding counterfeit Arkansas birth certificates that were known to have been used to obtain SSNs in that region. Nevertheless, the individual and his associates used versions of the same birth certificate to secure 956 additional SSNs from California FOs after that date.
- In February 1995, SSA issued a fraud alert in its Program Operations Manual System (POMS) to further warn FOs of counterfeit Arkansas birth certificates used to secure SSNs in California. Despite this additional guidance, California FOs issued 600 more SSNs to the individual and his associates after that date.
- The individuals obtained the SSNs at 119 FOs throughout California. At some of these offices, they obtained between 30 and 35 SSNs over the 4 ½-year period.
- Although the individual was arrested in August 1997 and this case was brought to the attention of SSA shortly thereafter, as of July 1998, only 7 of the 1,120 SSNs issued had been marked with a fraudulent special indicator in SSA systems.

OIG investigators who interviewed FO personnel at some of the 119 California FOs also noted a management control issue that they believed contributed to the individual's success in obtaining these SSNs. On numerous occasions when an employee questioned the validity of the individual's documents, the individual became defensive and rude. Obviously, FO personnel had the correct instincts in questioning the documents, but proceeded to approve the SSN applications. When questioned about their reactions, many cited that they did not want to offend the applicant. In short, their commitment to customer service and, perhaps, concern for their personal safety prevented them from confronting the potential fraud.

The individual was arrested in Los Angeles, California, on August 21, 1997, by OIG investigators. He subsequently pleaded guilty to one count of conspiracy and two counts of knowingly submitting false information to obtain a SSN. As a result, he was sentenced to 33 months in Federal prison, followed by 3 years of supervised probation.

The individual admitted to OIG investigators that he sold most of the fraudulently-obtained SSNs. We shared the information developed during our investigation with the

U.S. Secret Service/West African Task Force investigating a large credit card fraud ring. The task force investigators recognized over 60 names from the list of nonexistent children as defendants/suspects involved in the ring and estimated that these suspects were responsible for approximately \$30 million in credit card fraud. Further, we noted during our analysis that 27 of the 1,120 SSNs had been used by the individuals possessing the cards to work in the United States during 1997, even though these cards were supposedly issued for nonexistent children.

We acknowledge that this case is an atypically large representation of the type of SSN fraud encountered at SSA. Nevertheless, the actual scheme is not uncommon. In fact, we are currently investigating cases in Philadelphia, Pennsylvania, and Atlanta, Georgia, that are very similar to the one described above—though on a smaller scale. These cases illustrate several important control weaknesses within SSA's enumeration process. Specifically, the cases show that SSA's MES does not detect when: 1) the cumulative number of SSN applications made by a "parent" on behalf of his or her children exceeds a reasonable number; 2) multiple SSN cards are sent to a common address; and 3) known fraudulent documents are used as evidentiary documents with a SSN application. As such, we believe these cases provide an exceptional learning opportunity for SSA and should serve as a catalyst for changes essential to ensuring the integrity of the Agency's enumeration responsibility.

COUNTERFEIT ALIEN DOCUMENTS USED TO OBTAIN SSNS

SSA personnel are not always able to ensure the validity of documentation presented by aliens. As a part of our FY 1998 audit planning process, we contacted SSA officials from regional offices throughout the country to petition their audit suggestions related to the enumeration area. By far the most prevalent response we received related to the problem of false documents submitted by aliens when applying for SSNs. Respondents explained that despite the training and other tools available for FO use in verifying the documents, they simply cannot detect all of the fraudulent documents submitted with SSN applications. Accordingly, many respondents believed that more controls should be implemented to ensure the integrity of alien documents.

Our audit and investigative efforts have confirmed the concerns of SSA FO personnel. Although SSA has implemented numerous initiatives over the past few years to address the issue of fraudulent alien documentation, controls in this area are still not sufficient. Specifically, as described in the following paragraphs and as previously reported by the Department of Health and Human Services (HHS) and SSA's OIG, SSA's interface with INS' SAVE system is not effective.⁵ Although SSA is currently working to obtain an agreement with INS and the State Department that will allow the latter agencies to

⁵ HHS OIG reported problems with INS' SAVE program in its report, *Follow-Up Audit: General Accounting Office Report "Immigration Control: A New Role for the Social Security Card,"* issued in May 1991 (A-13-90-00039). Additionally, we addressed this issue in our report entitled, *Follow-up Review of the Internal Controls Over the Modernized Enumeration System,* issued in March 1998 (A-04-96-44001).

collect aliens' enumeration data and evidence, this initiative will not address process weaknesses for those aliens who choose to be enumerated at a SSA office.

Limitations in INS' SAVE Program

Despite its presumable value to SSA, INS' SAVE program has significant limitations that negate its usefulness. The intent of the SAVE program is to provide a method for SSA personnel to verify certain INS documents presented as evidence of lawful immigration status or work authority. However, the system is not a real-time resource and does not provide verification of all INS documents.

Because aliens require a SSN to work in the United States, most are very anxious to apply for and receive a number soon after entering the country. However, INS officials acknowledge that there is often a significant time lapse between the time an alien enters the country and the time that individual's information is available via the SAVE program. As such, SSA's POMS specifies that the SAVE program does not need to be used until after an alien has been in the United States for at least 30 days. Thus, for many of the aliens applying for SSNs, SSA FO personnel must rely on visual verification to determine the validity of alien documentation. Unfortunately, the technological advances available to create fraudulent documents exceed the advances in visual verification, often proving visual verification unreliable.

Additionally, the SAVE program does not provide a method to verify INS documents provided by nonimmigrants who are only temporarily visiting the United States and who were not assigned an employment authorization document. Some nonimmigrants are eligible to work while they are in the United States and are, therefore, entitled to a SSN. However, the SAVE program only provides a means to verify information provided by immigrants to whom INS assigns unique alien numbers. Accordingly, SSA must again rely on visual verification to ensure the validity of INS documentation provided by nonimmigrants.

Limitations of the SSA/INS/State Department Memoranda of Understanding

SSA, INS, and the State Department are currently working on agreements that will enable INS and the State Department to collect enumeration data from aliens upon their entry to the United States. Specifically, INS or the State Department will collect all of the information necessary to process a SSN application. INS will then forward the information to SSA for actual processing of the applications and issuance of the SSNs. SSA, INS, and the State Department have designed this process in an attempt to reduce fraud, improve customer service, and save administrative costs. The agencies believe that this initiative will significantly reduce the possibility of accepting counterfeit documentation and will eliminate duplicate contacts that aliens now must make in order to obtain SSNs. SSA further estimates that the Agency will save \$30 million in administrative costs over a 5-year period, as a result of this proposed arrangement.

We acknowledge the many benefits of this initiative and commend SSA for the proactive strides that it is taking to address the important issue of alien documentation fraud. Nevertheless, we do not believe that this arrangement will completely resolve SSA's documentation verification issue or negate the need for SSA to make changes in its process.

The most notable limitation that we have found in the agreements is that they do not require aliens to apply for SSNs through INS or the State Department. Rather, the agencies will offer this service to aliens eligible for a SSN. Aliens may choose to apply for their SSNs at a SSA office. Accordingly, problems that currently exist in SSA's documentation verification process will continue to be encountered by FO personnel even after the arrangement is implemented. Since illegal aliens cannot, in theory, apply for a SSN at INS or the State Department, SSA FO personnel may see a rise in the percentage of fraudulent documents presented and should be alerted to this phenomenon.

In summary, while we applaud the intent of the proposed agreement and acknowledge that SSA's workload in enumerating aliens will be reduced, we believe that circumstances still exist that necessitate changes in SSA policies and procedures.

Example of Counterfeit INS and Polish Documents Used to Obtain Over 250 SSNs

Since 1993, OIG with the assistance of INS has been conducting an investigation involving illegal Polish aliens who have obtained SSNs with false documentation. Investigators estimate that during the period 1993 to 1995, the Polish suspects obtained at least 250 SSNs from various SSA offices throughout the Midwest. Although investigators do not have comprehensive figures for the number of SSNs obtained after that date, they believe the suspects obtained many more from other SSA offices across the country. They perpetrated this scheme by using false INS documentation as evidence of lawful alien status. The suspects and illegal aliens that they assisted generally applied for the SSNs within 30 days after the entry date shown on their INS documents. Therefore, SSA personnel were unable to verify the documents presented after January 1997 through the SAVE program. In most cases, visual verification of the documents proved satisfactory for the FO personnel processing the applications.

Investigators believe that at least five Polish individuals are involved in the scheme. These five suspects smuggle Polish aliens into the United States through Canada and then escort the illegal aliens to SSA offices throughout the Midwest. The smugglers act as interpreters for the Polish aliens. Typically, the suspects and their accomplices apply for one or two SSNs (one for each) at each SSA office and have the cards sent to common mail drops around the country. It is believed that the suspects provided this service to Polish illegal aliens at a cost of approximately \$6,000 per individual.

So far during the investigation, SSA OIG and INS investigators made two arrests. They arrested the first individual in 1995 on charges that he provided a false statement on a SSN application. The court sentenced the suspect to the time that he served awaiting

trial and he was processed for deportation. However, he forfeited his bond money by failing to appear for departure. The investigators suspect that the individual may still be active in the alien smuggling ring.

Investigators made the second arrest in Denver, Colorado, in December 1998. The suspect was transferred to the Eastern District of Missouri for an initial hearing on January 11, 1999. After this hearing, the court released the suspect on bond and ordered him to appear at a preliminary trial on January 29, 1999. However, the suspect failed to appear for this hearing. U.S. Marshals are currently searching for the subject. Additionally, investigators continue to monitor SSNs issued to Polish aliens and sent to common addresses to determine whether the suspects are still operating the smuggling ring or may be a part of a larger organization.

Despite the investigators' efforts and the fact that many SSA offices in the Midwest areas have been warned to be on alert for counterfeit passports and INS documents presented by Polish SSN applicants, the suspects were successful in fraudulently obtaining over 250 SSNs.

Ongoing Audit Uncovered Numerous Potential Cases Involving Fraudulent INS Documents Used to Obtain SSNs

As a part of an ongoing OIG audit⁶ in which we are reviewing SSA's procedures for verifying evidentiary documentation submitted with original SSN applications, we have found numerous potential cases of SSN attainment using fraudulent INS documents. We will issue a separate report addressing specific findings resulting from this audit. Nevertheless, we believe that some of the preliminary results warrant the immediate attention of SSA management.

The objectives of this audit were to determine whether: 1) SSA's procedures for examining evidentiary documents are sufficient to ensure proper issuance of original SSNs, and 2) SSA personnel are complying with existing procedures. To accomplish our objectives, we visited 11 SSA FOs to observe and discuss documentation verification procedures. Additionally, we selected a sample of 5,389 SSNs that SSA sent to 90 addresses between September 1, 1997, and March 31, 1998.

To select this sample, we obtained a data extract from SSA's MES Transaction History File and identified addresses to which 10 or more SSNs were sent during the specified 7-month period. From a universe of 1,447 addresses and 32,964 SSNs, we then judgmentally selected 90 addresses that appeared most suspect for fraud based on several preliminary tests. We initially selected a sample of approximately 3,500 SSNs out of the 5,389 issued to the addresses for which we are attempting to verify the evidence presented. Additionally, we were unable to obtain verifications for over 400 applicants because SSA personnel did not record adequate descriptions of the evidence presented when processing the SSN applications or did not maintain the

⁶ "Review of SSA Procedures for Verifying Evidentiary Documents Presented With Original SSN Applications" (A-08-98-41009).

application. For the 3,500 SSNs, we are in the process of attempting to independently verify the evidence presented with each SSN application.

Although, we did not attempt to focus on SSNs issued to aliens when selecting our sample, 87 of the 90 addresses selected received SSNs almost entirely for aliens. As such, we have attempted to verify with INS the validity of the documentation presented to SSA. We have not yet received responses from INS on some of the information requested. Nevertheless, the following information presents some of the initial findings:

- At 16 of the 87 alien-related addresses, 99 percent of the SSNs that we were able to verify were issued as a result of false INS documentation. Specifically, 198 of the 201 alien registration numbers either 1) belonged to another alien or 2) had never been issued by INS. Our investigators are currently examining some of these cases. Other cases will be reviewed at a later date.
- Some of the addresses selected in our sample were refugee assistance organizations that had received hundreds of SSNs on behalf of the aliens they had assisted. In general, these agencies assist refugees entering the country in obtaining necessary documents (e.g., INS documents, SSNs) and in finding employment and housing. Our analysis indicated that, although, the majority of SSNs received by these agencies were based on valid documentation, some were not. For example, one notable refugee assistance organization received 236 SSNs during the specified period. Of these, 29 (12 percent) were supported by INS documents that could not be verified (i.e., the documents belonged to another individual or had never been issued by INS). Another organization received 90 SSNs, of which 12 (13 percent) were also based on invalid INS documentation.
- In California, we noted that 342 individuals, many of whom claimed to be nonimmigrant students of 1 university, received SSNs at 8 locations in the Los Angeles area. Some of these locations were individual apartments where up to 70 people received their cards. SSA regulations only allow nonimmigrant students to obtain a SSN if they have certain INS documents and can show that they plan to work on campus or in an off-campus training position. As such, we checked the earnings reports for those individuals receiving their SSNs in 1997. Only 6 (3 percent) of the 221 individuals who obtained their SSNs in 1997 had any earnings during that year. INS is currently attempting to verify the evidence that these individuals presented to obtain their SSNs.
- In the New York and New Jersey areas, we found that 183 nonimmigrants received SSNs at 10 locations throughout the area during the 7-month period reviewed. Again, most of these locations were apartments where up to 32 people received their cards. The nonimmigrants presented INS documents to SSA offices in the area indicating that, by their alien classifications, they were allowed to work while in the country. The unusual circumstance is that, while 25 people may have received their SSNs at 1 apartment, they had very differing alien classifications. For example, 1 apartment received cards for 32 nonimmigrants with R-1 (religious worker),

E-1 (treaty trader), P-1 (internationally recognized performer or athlete), and L-1 (intra-company transferee) alien classifications. All of the alien categories claimed by these individuals permit them to work in the United States. However, of the 137 SSNs issued to these addresses in 1997 (the remainder were issued in 1998), only 8 of the individuals (5.8 percent) had any earnings during that year.

IMPACT OF SSN FRAUD ON SSA PROGRAMS

We recognize that the monetary impact of SSN fraud on SSA's trust funds may not be extensive. All the same, unless measures are taken to reduce the incidences of identify fraud, the impact on SSA program integrity will continue to compound. As described in the following sections, we believe that SSN fraud and SSA's current regulations and policies toward this issue, have resulted in sometimes immeasurable consequences to SSA programs.

Conflict Between SSA's Strategic Goals

We recognize the sensitive balance that SSA must maintain between providing "World-Class Service" to its customers and ensuring enforcement of its "Zero Tolerance for Fraud" commitment. We also acknowledge that the public would not be tolerant if customer service were not a top priority. Nevertheless, we believe that SSA's implementation of these two goals sends contrasting messages to SSA personnel, especially those in FOs.

Although SSA personnel are provided training in fraud prevention and are asked to comply with certain procedures designed to prevent fraud, their performance is often measured in terms of customer service. At some offices we have visited during the course of our audits, FO personnel are extremely alert to the possibility of fraud and take precautions to prevent it from occurring. At many other offices, however, we found that SSA personnel circumvent some procedures in order to reduce the waiting time of customers. For example, we found that some personnel in FOs around the country did not use some of the document verification tools at their disposal (e.g., black lights, INS and Department of Motor Vehicle publications, SAVE) because they did not want the customers to have to wait excessive time periods while they accessed these tools.

In one instance, we found that management at a FO had attempted to implement additional fraud prevention procedures, but were instructed by the regional office to cease this process because it took too long for applicants to receive their SSNs. Specifically, for a period, the FO would not approve original SSN applications for any aliens until they could verify the aliens' INS documents through SAVE. As discussed in previous sections, this process sometimes took 30 to 60 days. Certain refugee assistance organizations and employers complained to the regional office about the length of the process. In response to the complaints, the regional office instructed the FO to discontinue this process. However, we found that one of the refugee

organizations that complained about the process received SSNs on behalf of aliens whose INS documents were not valid. Had the FO been allowed to continue with its process, these SSNs may not have been issued.

We believe that SSA should make it clear through its policies and performance measures that fraud prevention measures should never be circumvented to satisfy customer service. We support the measures taken by the FO and believe that SSA should consider adopting this policy. Given that INS and the State Department will begin collecting SSN information for aliens, we believe that for those aliens who choose to apply for a SSN at a SSA FO, the application should not be approved until their documentation has been validated by the issuing source.

Benefits Paid Inappropriately

Frequently, obtaining a SSN is a necessary first step for individuals planning to commit larger crimes. Although providing false information to obtain a SSN might not appear to have an impact on benefit dispensation, it is a “breeder” crime for financial fraud. Accordingly, when examining the crime of identity fraud, one must also analyze the intended purpose(s) for the crime. For example, using a fraudulently-obtained SSN provides individuals the opportunity to obtain SSA benefits for which they are not truly authorized. In one instance, OIG identified a New York resident who created 16 separate identities and obtained Supplemental Security Income benefits for each. As a result, the man collected \$561,346 in SSA benefits over an 8-year period. In a second example, an illegal alien used the SSN of another man to work in the United States and subsequently collect disability payments from SSA. Using the other man’s identity, the illegal alien collected \$246,540 in disability payments over a period of 17 years for which he and his family were not eligible.

We do not have specific figures quantifying the amount of SSA benefits paid to all individuals who have obtained SSNs fraudulently. However, we encourage the Agency to consider the ramifications to SSA’s trust funds.

Suspense File Postings

The intentional misuse of SSNs by individuals for work purposes has contributed to the enormous growth of SSA’s suspense file. When employers file annual wage reports that show workers’ names and SSNs that do not match SSA’s records, the earnings associated with these individuals are transferred to SSA’s suspense file. These earnings stay in the suspense file until employers, employees, and SSA can reconcile the discrepancies. Many of these items are often never resolved. In Calendar Year (CY) 1997, SSA’s suspense file contained approximately \$240 billion in earnings that had not been properly attributed to the correct individual. SSA estimates that almost 3.5 million items and \$20 billion are added to this figure annually.

Although poor employer reporting practices account for many of the wage items transferred to the SSA suspense file, it is believed that many suspense file items have

resulted from the intentional misuse of SSNs by aliens not authorized to work in the United States. Specifically, if aliens provide employers with either 1) a SSN that has never been issued, or 2) a SSN that SSA has already assigned to another individual, the earnings attributed to this alien will be transferred to the suspense file.

When attempting to resolve suspense file items, SSA performs a number of steps, including sending a letter to every employee or employer requesting information explaining the reason for the discrepancy. SSA also sends letters to employers who submit more than 10 percent of their annual wage reports with name and SSN discrepancies. In these letters, SSA describes to employers the importance of providing accurate employee information and details the penalties that may be imposed by the Internal Revenue Service for failing to do so.

Of the 6.5 million employers that report earnings to SSA in a given year, only 3 percent are considered major contributors to the suspense file. In fact, about 47 percent of all suspense items come from three industries: agriculture (17 percent), services (16 percent), and bars/restaurants (14 percent). SSA frequently performs outreach programs to such employers and SSA representatives provide instruction on how to ensure accurate wage reports. Additionally, SSA implemented the EVS program in an attempt to provide employers an avenue to verify employee information before the annual wage-reporting period. Through this program, employers can verify with SSA the SSN and name purported by each employee at the time the individual is hired. If SSA reports a name and SSN discrepancy to the employer, the employee is given the opportunity to remedy the error long before the annual wage report is submitted. If the information provided by the employee proves to be false, the employer has the opportunity to terminate the individual's employment. The EVS program is voluntary and currently used by only a small number of employers.

SSA Resources Currently Required to Address SSN Fraud

In addressing the issue of SSN fraud, SSA expends significant resources. For example, SSA expends resources to hire, train, and retain personnel who must spend a portion of every day working on issues related to SSN fraud. These individuals include, OIG investigators, Regional Security personnel, programmers, suspense file analysts, policy writers, public relations representatives, as well as FO employees. Again, the number of employees required to address this issue will compound unless SSA can implement more controls on the front-end to prevent SSN fraud from occurring.

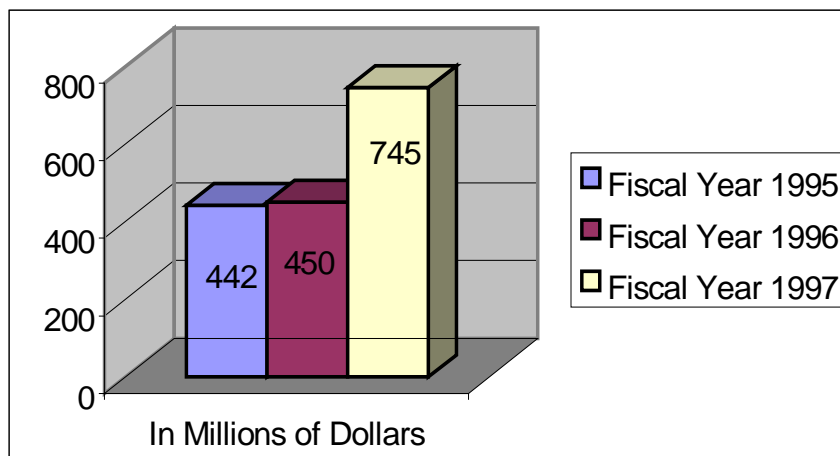
IMPACT OF IDENTITY FRAUD ON INDIVIDUALS AND ENTITIES EXTERNAL TO SSA

Frequently, national and local news reports illustrate crimes that have been committed using stolen or fraudulent SSNs. These crimes not only affect the Government's ability to administer its laws and programs, but also impacts individual citizens' attempts to receive and maintain satisfactory credit standings, as well as obtain other Government and private benefits. Additionally, identity fraud contributes to significant monetary

losses suffered by financial institutions and other Federal and State agencies. The following examples illustrate the impact of identity fraud on individuals and entities outside SSA.

- Although comprehensive statistics documenting the prevalence of identity fraud have not been accumulated, a 1998 GAO report quoted one credit bureau official as stating that two-thirds of all consumer inquiries to the company's Fraud Victim Assistance Department involve identity fraud. According to the official, the total number of inquiries increased from 35,235 in CY 1992 to 522,922 in CY 1997. The official attributed the trend to an increase in identity fraud as well as to the company's growth and outreach efforts.
- Officials at VISA U.S.A., Inc., and MasterCard International, Inc. reported to GAO that overall fraud losses from their member banks are in the hundreds of millions of dollars annually. Additionally, one official from MasterCard stated that dollar losses related to identity fraud represented about 96 percent of its member banks' overall fraud losses of \$407 million in 1997.
- As shown in the following chart, the U.S. Secret Service reported that “. . . actual losses—to the victimized individuals and institutions—associated with the agency's investigations of financial crimes involving identity fraud totaled \$442 million in FY 1995, \$450 million in FY 1996, and \$745 million in FY 1997.”

**Monetary Losses to Victims of Identity Fraud
Noted in U.S. Secret Service Investigations**



- GAO also reported that on an individual level, the “human” costs of identity fraud can be substantial. “These costs include emotional costs, as well as various financial and/or opportunity costs. For example, the victims may be unable to obtain a job, purchase a car, or qualify for a mortgage.”

CONCLUSIONS AND RECOMMENDATIONS

We believe that SSA must make both policy and procedural changes to ensure the integrity and security of its enumeration function. These changes will, in turn, help to reduce the number of instances in which SSNs are used to commit fraud. Further, the preponderance of SSN fraud cases discovered in recent years and the importance of SSNs in today's society gives weight to the following needed changes. We recommend that SSA:

1. Reemphasize to its employees that fraud prevention procedures should never be circumvented, irrespective of customer service demands. To its customers, SSA should use public relations vehicles to further communicate the Agency's commitment to fraud prevention.
2. Incorporate preventive controls in the MES that address the following circumstances: 1) multiple SSNs issued to a common address, 2) parents claiming to have had an improbably large number of children, 3) known fraudulent documentation used as evidence in support of SSN applications.
3. Require verification from the issuing State when an out-of-State birth certificate is presented as evidence for a SSN application.
4. Continue its efforts to have INS and the State Department collect and certify enumeration information for aliens.
5. Require that the FO obtain independent verification of an alien's evidentiary documentation from the issuing agency (e.g., INS, State Department) before approving the SSN application if an alien chooses to visit a SSA office to apply for his or her SSN.

AGENCY COMMENTS AND OIG RESPONSE

In its response, SSA recognized that the public's confidence in its stewardship of Agency programs is undermined when individuals succeed in abusing Agency systems. Additionally, the Agency acknowledged that instances of identity and noncitizen fraud have a significant societal impact. To address specific recommendations outlined in our report, SSA detailed numerous ongoing and future initiatives that it believed would correct identified weaknesses and reduce the possibility that similar cases of fraudulent SSN attainment will recur.

We acknowledge the steps SSA has taken and contemplated in attempting to combat SSN fraud and believe that the Agency's responses and planned actions adequately address two of our recommendations (recommendations 1 and 4). Nevertheless, we

believe the initiatives SSA cited to address the remaining three recommendations (recommendations 2, 3, and 5) will not effectively respond to our goal of **preventing** the fraudulent attainment of SSNs.

Recommendation 1

Reemphasize to its employees that fraud prevention procedures should never be circumvented, irrespective of customer service demands. To its customers, SSA should use public relations vehicles to further communicate the Agency's commitment to fraud prevention.

Agency Comments:

SSA plans to issue a reminder to FO personnel regarding the importance of adhering to fraud prevention procedures, irrespective of customer service demands. Additionally, SSA plans to review current public relations vehicles and explore opportunities to reemphasize to the public the importance of fraud prevention activities.

OIG Response:

SSA's planned actions adequately respond to this recommendation.

Recommendation 2

SSA should incorporate preventive controls in its MES that address the following circumstances: 1) multiple SSNs issued to a common address, 2) parents claiming to have had an improbably large number of children, and 3) known fraudulent documentation used as evidence in support of SSN applications.

Agency Comments:

In responding to this recommendation, the Agency cited three initiatives that it believed addressed integrity concerns within the enumeration system. First, as required by the Taxpayer Relief Act of 1997, SSA now obtains and forwards to the IRS the SSNs of parents who apply for original SSNs on behalf of their children under age 18. As parents will no longer be "anonymous," SSA expects that this requirement will serve as a deterrent. Second, SSA sends a semiannual report to the OIG identifying instances in which 10 or more SSNs are sent to the same address within a 6-month period. SSA stated that it will also work with the OIG to more effectively target potential fraudulent activity. Third, SSA began using a new version of its Comprehensive Integrity Review Program to identify instances in which four or more cards are sent to the same address within a 5-week period. FOs are alerted to these instances and required to perform preliminary investigation on these occurrences.

OIG Response:

The initiatives that SSA proposed in response to our recommendation appear to concentrate on the **detection** of fraud after it has already occurred. Unfortunately, once a SSN has been issued, SSA has little ability to prevent or curtail the use of that SSN in committing further fraud. We recognize that not all fraud committed using SSNs negatively impacts SSA trust funds. Nevertheless, we believe SSA must hold itself accountable for **preventing** SSNs from being obtained through illegal means and used to the detriment of other elements within our society. As suggested in our recommendation, we believe the Agency's initiatives should focus on front-end controls within MES that will preclude the issuance of SSNs in certain defined circumstances. We do not believe that the initiatives SSA described adequately incorporate these preventative controls.

Although Federal law and SSA policies now require parents to provide their own SSNs when applying for SSNs on behalf of their children, SSA controls still do not prevent SSNs from being issued when parents claim to have an improbably large number of children. For example, even under this new law, the individuals in the California case cited earlier in this report would have been successful in obtaining 1,120 SSNs for nonexistent children because they had accurate SSNs for each of their aliases. To prevent recurrences such as this, SSA needs to program MES to track the number of children per parent (via the parent's SSN) and notify the applicable FO **before** issuing further SSNs when the number becomes improbable. This same concept should be applied to multiple SSNs that are sent to a common address.

We also point out that SSA's response did not address our recommendation that controls be instituted preventing the issuance of SSNs based on known fraudulent documentation. One of the most disturbing facts identified in our investigation of the California case was that hundreds of SSNs were issued for nonexistent children long after the regional office and SSA published fraud alerts regarding the Arkansas birth certificates used to obtain these numbers. Obviously, the fraud alerts did not gain the proper attention of personnel processing these applications. As such, we continue to believe that SSA needs an automated mechanism or control that will prevent SSNs from being issued if a known fraudulent document is used.

We encourage SSA to reconsider its response to this recommendation.

Recommendation 3

SSA should require verification from the issuing State when an out-of-State birth certificate is presented as evidence for a SSN.

Agency Comments:

In its response to our report, SSA asserted that requiring independent verification of out-of-State birth certificates that are presented as evidence for SSN applications would be impractical for the public and SSA FOs. However, the Agency cited another initiative that it is contemplating for future years. Specifically, SSA hopes to gain on-line access to State vital records data so that FOs can verify birth and death records provided by SSA customers.

OIG Response:

The implementation of this initiative is contingent on obtaining agreements with all of the States and jurisdictions—first for accessing in-State data and then separate agreements so that data can be shared across State lines. While this goal will certainly prove worthy in the future, implementation may be years away. In the meantime, we believe SSA should reconsider our recommendation to independently verify out-of-State birth certificates. Given the reduction in newborn SSN applications processed by FOs as a result of the enumeration-at-birth process and the infrequency that out-of-State birth certificates are presented with SSN applications, we do not believe that this requirement is impractical.

We encourage SSA to reconsider its response to this recommendation.

Recommendation 4

Continue its efforts to have INS and the State Department collect and certify enumeration information for aliens.

Agency Comments:

SSA plans to continue its efforts to have INS and the State Department collect enumeration information for noncitizens and is in the process of working out the final details of these arrangements.

OIG Response:

SSA's planned actions adequately respond to this recommendation.

Recommendation 5

SSA should require that the FO obtain independent verification of an alien's evidentiary documentation from the issuing agency (e.g., INS, State Department) before approving the application if an alien chooses to visit a SSA office to apply for his or her SSN.

Agency Comments:

In its response, SSA stated that it planned to be vigilant in its efforts to guard against the submission of fraudulent documents by aliens applying for SSNs at FOs. Additionally, the Agency is working with INS to improve and shorten the current document verification process. However, the Agency did not agree to obtain independent verification of alien documents.

OIG Response:

We do not agree with SSA's response to this recommendation. Although we are confident that SSA has been and will continue to be vigilant in its attempts to prevent the acceptance of fraudulent alien documents, as evidenced by the cases presented in this report, current SSA procedures have not always been successful in this endeavor.

We acknowledge SSA's efforts in working with INS to improve and shorten the verification process (e.g., the time lag in INS' SAVE system). However, we have held our own conversations with INS personnel and believe that the INS system improvements necessary to effect positive changes within SSA's verification process will take many years to implement.

Again, we believe it is imperative that SSA institute controls to **prevent** the issuance of SSNs based on fraudulent documents. By doing so, the Agency can ensure that it is doing its part to control the growing identity fraud trend. Until such time as alien documents are independently verified by the issuing agencies, we do not believe SSA can accomplish this goal.

We encourage SSA to reconsider its response to our recommendation.

SSA also provided technical comments that have been considered and incorporated, where appropriate, in this final report. The full text of SSA's comments is included in Appendix A.

APPENDICES

SSA COMMENTS

MAJOR REPORT CONTRIBUTORS

Office of the Inspector General

Office of Audit:

Gary Kramer, Director, Program Audits (East)
Kim Byrd, Senior Auditor
Cheryl Robinson, Writer-Editor, Technical Services

Office of Investigations:

Mike Kowal, Assistant Special Agent-in-Charge, Strategic Enforcement Division
David Butler, Assistant Special Agent-in-Charge
Sal Grasso, Special Agent

For additional copies of this report, please contact the Office of the Inspector General's Public Affairs Specialist at (410) 966-9558. Refer to Common Identification Number A-08-99-42002.

SSA ORGANIZATIONAL CHART
