U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Oversight
Subcommittee on Social Security

Statement for the Record

Social Security Number and Individual Taxpayer Identification Number Mismatches and Misuse

Patrick P. O'Carroll, Jr.
Acting Inspector General, Social Security Administration

March 10, 2004

Good morning, it is a pleasure to be here today for this important hearing on the issues of Social Security number (SSN) and Individual Tax Identification Number (ITIN) mismatches and misuse. Today's discussion will provide valuable insight into the impact and implications that ITINs have across the Federal government. Today, I would like to focus my comments on the ITIN's impact on the Social Security Administration's (SSA) programs and operations.

SSA's Office of the Inspector General (OIG) has worked very hard with the Agency in recent years and made significant progress to strengthen the defenses of the SSN. These activities included close cooperation with other law enforcement agencies and with the Internal Revenue Service (IRS) to strengthen the integrity of SSA's data and those who rely upon it.

Over the past few years, we have testified on numerous occasions before Congress on the topics of SSN misuse, document fraud, and identity theft. The most important aspect of our mission to combat fraud, waste and abuse is the protection and oversight of the SSN. Today, the SSN is the single most widely used identifier for Federal and State governments, as well as for the private sector. As a result, we continuously seek new and innovative ways to prevent SSN misuse and work collaboratively with other Federal, State, and local entities. Although we have made notable progress, the public's reliance on the SSN as a national identifier has made it an increasingly valuable commodity for lawbreakers trying to take advantage of SSA's programs and operations.

Similarly, the growth and misuse of ITINs pose considerable challenges for SSA. Today, I will highlight three areas and provide an overview of our work to address these challenges. First, I will discuss the ITIN's impact on SSA's earnings process. Second, I will summarize the ITIN's impact on SSN misuse and identity theft. Third, I will outline our most serious concern, how misuse of the ITIN or SSN could impact Homeland Security. I will conclude my remarks with a brief summary of recommendations to improve these processes and outline opportunities to open a broader dialogue on these issues.

The ITIN's Impact on SSA's Earnings Process

As mandated by Title II of the Social Security Act, SSA maintains records of wage amounts employers pay to individuals. Each year, employers and self-employed individuals report earnings information to SSA using a unique nine-digit number, the SSN. This information is used to determine (1) whether an individual is eligible for retirement or disability benefits and (2) the size of the benefit payment. Accordingly, it is critical that SSA protect the integrity of the SSN and properly post wages reported through the Agency's earnings process.

SSA has no role in assigning ITINs. This function is the sole responsibility of the IRS. Nevertheless, IRS use of these numbers may negatively impact SSA's ability to accurately record employee wage information. Because the nine-digit ITIN so closely resembles an SSN, many employers assume it is an SSN. Yet when employers report wages earned by an individual to SSA using the IRS ITIN rather than the individual's SSN, SSA is unable to post these earnings to the wage earner's record.

When SSA is unable to post earnings to an individuals' record, the earnings are captured in SSA's Earnings Suspense File (ESF), the Agency's record of wage reports for which wage earner names and SSNs fail to match SSA's records. Although SSA is able to post about 96.4 percent of all reported earnings to individuals' earnings records, those earnings that cannot be matched continue to accumulate in the ESF. Between 1937 and 2003, the ESF grew to about $421 billion in wages, representing about 244 million wage items that could not be posted correctly.

Removal of wage items and their associated dollar value from the ESF occurs only when the wages can be matched and posted to an individual's master earnings file. Since the Agency does not enumerate the owners of ITINs, its ability to match these wages correctly will be even more difficult because SSA has incomplete information on the ITIN holder.

Still, while SSA has limited control over the factors that cause the volume of erroneous wage reports submitted each year, the Agency does have some ability to improve the wage reporting process. SSA can work with employers to resolve wage reporting issues, encourage greater use of SSN verification programs, and improve coordination with other Federal agencies such as the IRS that have separate yet related mandates, to foster better sharing of information.

Additionally, we believe increased coordination between SSA, IRS and DHS could be used to detect trends, identify problems in the employer community and to pro\pose legislative remedies. For example, cooperation between IRS and SSA on the ITIN process could minimize the volume of incorrect wages posted to the ESF.

The ITIN's Impact on SSN Misuse and Identity Theft

It is no longer realistic to believe that the SSN is simply a number for tracking workers' earnings and the payment of social insurance benefits. Recognizing the importance of the SSN throughout society, SSA has taken significant steps to strengthen controls over the issuance of SSNs in recent years. We applaud SSA's efforts, but we are concerned that increased misuse of ITINs may undermine some Agency initiatives.

In FY 2001, SSA established a task force to address SSN integrity concerns, and took a number of important steps. For example, in September 2002, SSA started independently verifying all non-citizen immigration documents prior to issuing an SSN. We are currently assessing the Agency's compliance with these new procedures. However, we do not know whether IRS takes similar measures when issuing ITINs to non-citizens.

SSA also recently restricted the issuance of non-work SSNs to non-citizens except under very limited circumstances. Under this policy, non-citizens should only be issued a non-work SSN because:

- Federal statute or regulation requires that the non-citizen provide his or her SSN to get the particular benefit or service, or
- State or local law requires that the non-citizen provide an SSN to get general assistance benefits to which the non-citizen has established entitlement.

As a result of SSA's new policy regarding non-work SSNs, the use of ITINs for work purposes may increase. Non-citizens in the United States without work authorization who were previously able to use non-work SSNs for tax purposes may now obtain an ITIN and present it to a prospective employer as an SSN and use it instead for wage reporting.

Currently, there are several provisions of the law that address SSN misuse, such as:

- Social Security Act provisions that make it a felony to deliberately represent another person's SSN as your own.
- Identity Theft and Assumption Deterrence Act provisions that make it a criminal offense to knowingly use another person's means of identification with the intent to commit a violation of Federal law. This would include using another individual's personal identifying information, such as an SSN, or providing that SSN to obtain a tax refund.

We applaud the recent announcement by IRS that it will discontinue its practice of issuing ITINs in the form of cards, and instead will notify ITIN applicants by letter. However, we fully expect that the growing confusion between ITINs and SSNs will exacerbate problems with wage reporting. Additionally, the ease with which one obtains an ITIN may negate the robust screening processes used to deter fraudulent applications.

For example, we have found that the ITIN has been used to facilitate fraud in cases where an ITIN is submitted as if it were an SSN. In one such case, a woman using an ITIN as her SSN obtained loans and lines of credit of approximately $300,000. Furthermore, she was able to secure a mortgage of nearly $140,000 by furnishing bogus W–2 forms bearing the ITIN.

ITIN/SSN Misuse Impact on Homeland Security

Still, while financial crimes involving SSNs are more numerous than terrorism-related crimes involving misuse of the SSN, the potential threat SSN misuse poses to homeland security is also of real concern.

The information SSA stores on each of us is personal, and is entitled to all of the protections we can afford. However, I have learned during my role leading OIG's investigative effort, that there are times when an individual's privacy must be balanced against the need of law enforcement agencies for information to protect our country. For example, following September 11th, and again during the sniper attacks in the Washington, D.C. area, it became necessary to share information stored by SSA with appropriate law enforcement authorities to permit those authorities to conduct their investigations and, more importantly, prevent additional lives from being lost.

On both occasions, we asked to use the ad hoc authority vested in the Commissioner by SSA regulations to permit the sharing of SSA information with our law enforcement partners. However, we believe in instances like this the Inspector General of Social Security should have the ability to disclose such information without prior approval. When lives are at stake, every minute is critical, and we need to be able to provide this information as expeditiously as possible.

Those connected with terrorism will at some point either take advantage of security gaps across the Federal government or try to obtain SSNs or ITINs. They may seek SSNs or ITINs through:

- The use of counterfeit or stolen documents purchased on the Internet or created through readily available computer processing equipment and software.
- Fraudulent application for genuine documents issued by government agencies.

Therefore, we must remain vigilant to ensure that there are adequate safeguards to prevent the misuse of SSNs and ITINs.

We believe the misuse of ITINs could undermine SSA's programs and our investigative ability to provide reliable data to the law enforcement community. ITINs could be used to facilitate an underground network to undermine homeland security and perpetrate fraud against our economy and its citizens. It is incumbent upon us to resolve these issues now, before another crisis emerges and data is needed quickly.

Nationally, OIG has been an active participant on Joint Terrorism Task Forces. We have provided round-the-clock support to the national criminal investigation of potential terrorist activities. Our special agents and attorneys have helped identify, detain, indict, and convict individuals who may have a relationship with terrorist activities. For example, we have investigated airport employees during our homeland security operations who used ITINs on applications to obtain Secure Identification Display Area badges.

Additionally, our Electronic Crime Team rendered assistance to the FBI, while our computer specialists wrote programs to more specifically query SSA's databases for FBI-requested information. Many of our investigators continue to perform substantial work on terrorism investigations and respond to allegations of SSN misuse.

Many of our agents participated in Operation Swipe Out, a large-scale, anti-terrorism, white collar crime initiative. The investigation focused on the fraudulent activities of a Pakistani group involved in credit card, Social Security, immigration, bank and mortgage fraud. Starting in January 2003, 30 criminal complaints/arrest warrants and two search warrants were issued. The

suspects defrauded numerous credit card companies of approximately $5 million, sending some of their proceeds to banks in Pakistan and Canada. For the 30 criminal cases, 17 of the subjects pleaded guilty, receiving sentences ranging from 2 years probation to 57 months of incarceration, and being ordered to pay $1,137,224 restitution. Two subjects' cases were dismissed; the remaining 11 subjects are fugitives. Seven were charged with SSN misuse.

In other situations, criminals 2 "shop" for State and local governments that do not mandate an SSN, and consequently accept an ITIN. One of our investigations detected an SSA employee furnishing SSNs to a co-conspirator who supplied them to illegal aliens for obtaining driver's licenses. After the employee was arrested and no longer able to provide SSNs, the co-conspirator simply moved his operation to North Carolina, which allowed the use of ITINs for driver's licenses.

In a 2002 audit, we discussed our concerns regarding SSA's risk of exposure to improper enumeration of foreign students. We found SSA did not have a reliable system for determining whether a foreign student is actually enrolled at an educational institution and required an SSN to perform authorized work. Some schools provided work authorization letters to students for on-campus employment when the school had not actually extended an employment offer to the student. As a result of our recommendation, the Agency proposed a regulatory requirement that evidence of actual employment be necessary for foreign students to receive SSNs.

In a draft report we recently issued to SSA, we reported that at least 22 colleges and universities across the country—9 of which represent those with the largest foreign student populations—advertise on their web sites that they will issue ''temporary SSNs'' to students. These numbers are not issued by SSA, but are generally nine-digit numbers that resemble an SSN or an ITIN. One university even provided the names of several banks where foreign students could open a bank account with one of these ''temporary SSNs.'' We are recommending that SSA contact these universities and discourage them from continuing this practice. We are also recommending that SSA work with national education committees and alliances to spread the word that this practice should be halted.

Areas for improved coordination

The areas that need improved coordination are:

- Sharing of data.
- Data reliability.
- Use of shared data.

SSA maintains two types of information in its databases; 1) SSA information received from individuals self-reporting on applications for SSNs or Social Security benefits, or from States and the private sector; and 2) IRS information received from employers in the form of W–2s and W–3s.

IRS maintains information in its databases generally from W–2s, W–3s and tax information. However, Section 6103 of the Internal Revenue Code restricts (with exceptions) the disclosure of this information to any other Federal, State, or local agency.

Currently, IRS already releases taxpayer data for statistical purposes to the Department of Commerce's Bureau of Economic Analysis and similar organizations, indicating that such data can be released for legitimate governmental purposes. However, further opportunities for expansion of coordination should be explored to allow for joint pilots and/or non-investigative reviews to allow auditors to identify areas where formal disclosure agreements could be later negotiated if warranted.

For example, SSA shared data with IRS on the 100 employers having the most wage items in suspense. This information could assist IRS to assess penalties against these employers for reporting mismatched names and SSNs on W–2 forms. SSA is also cooperating with DHS on unauthorized workers in the U.S. economy. Each year SSA sends DHS information on over 500,000 individuals who are not authorized to work in the U.S. economy, but who nonetheless show wages in SSA's system. A recent report we issued, "Profile of the Social Security Administration's Non-work Alien File," found DHS is neither using this information to take action against these individuals nor advising SSA when they are authorized to work in the U.S. economy.

It is imperative that SSA and IRS have consistent and reliable information to improve efficiency and effectiveness, and to reduce fraud, waste and abuse. While SSA is already actively sharing its own data with other agencies, there are a number of one-way restrictions and boundaries by law that limit the sharing of data between IRS and SSA. We are working with IRS to improve data reliability. Despite the restrictions I have outlined, we stand ready to work with IRS and DHS to develop strategies to improve our collective ability to use existing information to ensure the integrity of the SSN and strengthen homeland security.

For example, we believe the following combined efforts would enable both agencies to make significant strides in addressing the ITIN/SSN misuse issue.

- Improved Employee Verification
- Cross-Verification of Data

Improved Employee Verification

Coordination with IRS on employee verification would assist employers with one-stop verification of employee data. SSA already assists employers with its Employee Verification Service (EVS) for registered employers.

SSA is also piloting an online Social Security Number Verification Service (SSNVS), which allows employers and third parties to verify employees' names and SSNs via the Internet with information in SSA's records for wage reporting purposes. As with EVS, SSNVS also provides a death indicator where SSA records indicate that the employee is deceased. Employers have two online options to use SSNVS:

- Key in up to 10 names and SSNs at a time and the results are returned in seconds.
- Submit a file containing up to 250,000 names and SSNs per file and the results are returned the next business day.

SSNVS is beneficial because it:

- Helps employers use correct names and SSNs on wage reports.
- Reduces the number of submission errors.
- Offers an additional method of requesting verification services.
- Reduces the number of telephone calls required for employers to verify names and SSNs.

Cross-Verification of Data

Cross-verification would improve the process without requiring major expenditures of money or the creation of new offices or agencies. We believe legislation is needed to require mandatory cross-verification of identification data between governmental, financial and commercial holders of records and the SSA on a recurring basis. Much of the data already exists and could be drawn from information the Federal, State and local governments and the financial sector already have.

All options should be explored to make the cost of providing this service budget neutral. The technology is already in place to allow these data matches and verifications to take place. Coupled with steps underway by SSA to strengthen the integrity of its enumeration business process, cross-verification would be an important step to help prevent the spread of SSN misuse and identity theft, and to improve homeland security.

Some possibilities for cross-verification are:

- Mandatory SSN verifications for employees in critical or sensitive positions, such as defense, energy, chemicals, transportation, and national security.
- SSN verification for banks, credit reporting agencies and other financial lending institutions.
- The ability to verify SSN data for all law-enforcement entities.

Another positive aspect of cross-verification for SSA is the ability to correct errors on a more timely basis—errors that might otherwise keep workers from receiving full credit for years of labor and credit that can be nullified by simple typographical errors in submitting their data.

Conclusion

I want to congratulate Congress, and especially Chairman Shaw and Ranking Member Matsui, on the recent enactment of H.R.743, the Social Security Protection Act of 2003. This milestone bill, the work of three Congresses, provides new safe□guards for Social Security and Supplemental Security Income (SSI) beneficiaries who have representative payees, and will enhance other program protections. It will also provide significant new authority to our office to protect the SSN, SSA employees, and the Social Security Trust Funds.

The challenge for Congress and SSA is to balance the SSN's privacy against public and private needs to have limited access to this data. In the spirit of H.R. 2971, Chairman Shaw's pending SSN legislation, we believe the following steps need to be taken to meet this challenge:

- Limit the SSN's public availability to the greatest extent practicable, without unduly limiting commerce.
- Prohibit the sale of SSNs, prohibit their display on public records, and limit their use to valid transactions.
- Enact strong enforcement mechanisms and stiff penalties to further discourage SSN misuse.
- Cross-verify all legitimate databases that use the SSN as a key data element.

We are cognizant of the legal restrictions regarding the sharing of data, and respect the right to protect individual privacy concerns, however, we believe greater coordination and controlled sharing of data will improve the integrity of the SSN and SSA's programs.

I thank you for your continuing commitment to these critical issues, and would be happy to answer any questions.