

## ISPEECH

# Immigration Enforcement and Social Security: An IG Perspective

*Every year SSA receives 245 million wage reports from employers representing 4 trillion dollars in earnings*

**BY INSPECTOR GENERAL  
PATRICK P. O'CARROLL**

*Condensed from a speech delivered by Patrick P. O'Carroll, Jr., Inspector General for the Social Security Administration, on November 18, 2008 at a Federal Bar Association seminar, Worksite Enforcement and Immigration, Loyola University, Chicago, Illinois.*

It's a pleasure to be here with you in Chicago, and I'm honored to have been asked to speak. You've had a lot of excitement here in Chicago lately, from the Cubs' run for the World Series to a native son's first appearance as President-elect. I can't compete with such momentous events, but I do hope to give you an understanding of how the mission of my office intersects with the topic of your conference—workplace enforcement and immigration.

The federal government, with its nearly 3 million-strong workforce can feel somewhat amorphous, with only vague distinctions between one agency and the next. The truth, however, is that Congress has done a good job of giving Executive Branch agencies their own patches of earth to tend, so to speak.

For the Social Security Administration, that patch of earth is administering the programs enacted by the Social Security Act in 1935—as well as programs added to that mandate in the years since. One critical component of that mission involves the integrity of the Social Security number, or SSN. And as the uses of the SSN have expanded over the years, so has the number of places in which our



mission intersects with the missions of other agencies.

Today, we're discussing immigration, and where our jurisdiction intersects with that of Immigration and Customs Enforcement. But we could just as easily be talking about identity theft, where we intersect with the Federal Trade Commission, disaster-related fraud (such as in the wake of Katrina), where we intersect with FEMA, or any number of other areas in which the SSN is in play.

Before I go too far, though, I want to start by placing this discussion in context. I realize that some of you may not be familiar with the role of an inspector general or with our organization specifically. Then I'll zero in on how we work with the Social Security Administration, or SSA, and other agencies to combat SSN misuse in all of its forms, including

in the context of immigration and worksite enforcement.

Federal inspectors general serve as watchdogs over Executive Branch agencies, in an effort to increase public accountability and transparency in Government operations. Our mission is to help improve our agencies' programs and operations by conducting audits and investigations aimed at preventing and detecting fraud, waste, and abuse.

The Office of the Inspector General, or OIG, for SSA was created in 1995, when SSA became an independent Federal agency, separate from the Department of Health and Human Services. Today we are a team of 575 auditors, investigators, attorneys, and others which produced over 100 audit reports and closed over 10,000 investigations last fiscal year.

These are big numbers—but let me put

those accomplishments in perspective. We oversee an agency that manages the largest social insurance program in the world. Last year, SSA paid 614 billion dollars to over 50 million people. Our challenging mission is to protect and improve SSA's already well-oiled machine.

Each year, we receive upwards of 100,000 allegations of Social Security-related fraud, and I mentioned that last year, we closed over 10,000 investigations. Only about 9 percent of those cases were classified as Social Security number misuse, while 70 percent were related to fraud in SSA's disability programs—both Disability Insurance, which is an earned benefit, and Supplemental Security Income, for low-income disabled individuals.

Nevertheless, SSN misuse has certainly been one of our most enduring challenges over the 13 years of our existence. Despite its relatively smaller share of our caseload, maintaining the integrity of the Social Security number remains a key part of our mission, because of its role as the cornerstone of SSA's programs and operations.

This 9-digit identification number was created in 1936 for only one purpose: to uniquely identify individuals so that SSA could accurately track their earnings and contributions, and pay them benefits when the time came. Of course, we all know that today, Social Security numbers are used for much more than that original purpose. You are just as likely to have to supply your SSN to go to the doctor or buy a cell phone, as to report income to the IRS and Social Security or apply for retirement benefits.

As identity theft appeared on the horizon and became the crime of the new century, we found ourselves investigating more and more SSN misuse cases that had no true bearing on SSA's programs and operations. In recent years, however, I've led the OIG in an effort to focus our resources on combating only that SSN misuse which is directly linked to SSA's programs and operations.

We now generally refer identity theft allegations to those Federal, State and lo-

cal law enforcement agencies which have taken the lead on fighting bank fraud, mail fraud, and other identity theft crimes not directly related to Social Security. This refocusing of our resources has allowed us to more specifically target SSN misuse that directly affects SSA's programs and its beneficiaries. For example, we often find that individuals will misuse SSNs in connection with receiving government assistance, medical services, or other benefits.

Over the last 3 years, for example, we have participated on a Department of Justice task force dedicated to combating fraud related to Hurricanes Katrina and Rita. In the storms' wake, many individuals took advantage of the chaotic situation and defrauded disaster assistance programs. There were people who claimed they were living in a hurricane-affected area when they never had. Some individuals filed dozens of false claims using made-up names and SSNs. And many cases involved pure identity theft—someone pretending to be another individual who rightly deserved the funds.

Most of these cases involved some degree of Social Security number misuse, and we also found that many of those suspected of fraud against FEMA and HUD were also Social Security beneficiaries or SSI recipients. As a result, we have been involved in a number of task force investigations. Overall our hurricane fraud investigations have led to 52 convictions and the recovery of significant government funds.

Of course, Social Security number misuse also occurs for the purpose of obtaining a job in the United States. The need to maintain the accuracy and integrity of SSA's records gives the OIG a stake in identifying and preventing this type of SSN misuse. In fact, I believe our efforts are critical to maintaining the integrity of the entire Social Security system. That's because the system is based on SSA's ability to match workers' earnings to their Social Security records, so that when those workers become disabled or retire, they will receive the monthly

benefits they have earned.

Every year, SSA receives 245 million wage reports from employers, representing 4 *trillion* dollars in earnings. Americans must be confident in the knowledge that SSA will correctly record those earnings, and that they will get the full benefits due them. When earnings are incorrectly recorded, the individual worker and all taxpayers bear the cost of getting the record corrected.

Our work in this area reaches in many directions, and one of those paths intersects with the mission of Immigration and Customs Enforcement at the Department of Homeland Security. When employers or self-employed people report earnings on a W-2 form or 1099, SSA validates the name and Social Security number against its own records. When an earnings report contains a name or SSN that does not match SSA's records, and the discrepancy can't be resolved, SSA posts those earnings to a virtual repository known as the Earnings Suspense File, or ESF.

Sometimes the error is due to a simple discrepancy in SSA's records—for instance, when a woman marries and changes her name, but neglects to notify SSA. If her employer reports her wages under her new name, that name won't match up with her SSA record, so the Agency may post those earnings to the ESF. Of course, sometimes these errors are caught by the beneficiary, and the earnings record can be corrected.

However, most wage items remain in the ESF. As of October 2006, the ESF had accumulated about 586 billion dollars in wages and 264 million wage items. This creates an enormous resource drain for SSA and creates the risk that untold numbers of individuals will not receive the benefits they are due at retirement, upon becoming disabled, or as the result of another life-altering event.

We have conducted substantial audit work related to the Earnings Suspense File, in an effort to understand why wage reports end up in the file. The most well-known of those audits came up with a list of 100 employers with the most wage



items in the ESF, and analyzed those items for errors or SSN misuse. We found that many of the 100 employers were in the service, restaurant, and agriculture industries. We also found that SSN misuse seemed to be the reason for most of the mismatched records.

We then conducted an audit focusing on just the service, restaurant, and agriculture industries. We analyzed a sample of the wage reports in the ESF that were submitted by employers in these industries. Twenty-five percent of the SSNs had never been assigned, and 75 percent belonged to someone else—in fact, many belonged to young children or deceased individuals. That audit also found that 48 percent of wage items contributed by agricultural employers during the three-year period we reviewed failed to match SSA records.

Thus, while many of the ESF entries may be the result of simple error, we believe that the main contributor to the ESF is unauthorized work by noncitizens. Unfortunately, we also determined that there's little SSA can do to stem the tide of erroneous wage reports. Although we recommended that SSA assist IRS in developing an employer penalty mechanism, we're not aware that any such effort has been undertaken.

To this point, I've spoken about employment-related SSN misuse in general, but that broad term encompasses many variations. An individual may create an SSN out of thin air to supply to an employer, or use a deceased or living relative's number, or they may have bought a fake Social Security card on the street. In rare instances, they may have even acquired a genuine number from an SSA employee.

When an unauthorized worker uses an SSN that belongs to a living individual, that individual and SSA face administrative challenges in getting his or her earnings record corrected. And if the error is never caught or the record corrected, the true number holder may be paid the wrong amount of benefits, which over a lifetime could mean millions of dollars lost to taxpayers.

Another administrative challenge is posed by the fact that any unauthorized worker who later becomes authorized to work can go to SSA and request that wages in the ESF be attached to his or her earnings record. So even though the wages were earned and reported under another SSN, that person can qualify for benefits if they can prove that they earned the wages and are now authorized to work.

In light of the direct impact on SSA programs and operations, we do choose to participate with ICE to a very limited extent in worksite enforcement investigations related to employment-related SSN misuse. Specifically, we choose to participate only in those worksite enforcement operations where an employer is complicit in providing its workforce with fraudulent SSNs.

These employers harm the integrity of not only Social Security's records, but also its operations, by intentionally reporting false information year after year for dozens or even hundreds of individuals, and sometimes even by supplying counterfeit Social Security cards.

Even in those investigations we join, the OIG's role is often limited. But when we can stop employers from providing workers with fictitious SSNs or the SSNs of other people, the impact on SSA programs and operations can be significant.

In one egregious case, ICE requested our assistance with an investigation of a Boston company with a Department of Defense contract worth 100 million dollars. This company manufactured, among other things, bulletproof vests and backpacks for military personnel in Iraq and Afghanistan. ICE suspected the company's owner and plant managers of conspiring to hire unauthorized workers on a large scale.

We joined the ICE investigation, and in reviewing SSA's records, we found that over five years, the company had repeatedly failed to respond to SSA's correspondence informing them of erroneous wage reports. What's more, they never took any corrective action to prevent the

misuse. We discovered that up to 85 percent of the company's employees were using SSNs not assigned to them by SSA. As ICE pursued 360 unauthorized workers, our agents sought out and arrested the company's owner and three managers for conspiracy.

We also arrested a previously deported man who was running a counterfeit document enterprise out of a Boston-area storefront. The company was referring workers to the counterfeiter to obtain false documents that the company then accepted for hiring and wage-reporting purposes. The counterfeiter eventually pled guilty and was sentenced to time served, and transferred to ICE for deportation proceedings. The company's owner and managers also pled guilty and are awaiting sentencing in Federal court.

As you can see, our agents often find themselves working to combat document fraud, which can go hand-in-hand with SSN misuse. Unfortunately, there is a profit to be made by counterfeiting Social Security cards and immigration documents and selling them to unauthorized workers. As a result, the SSA OIG participates on ICE's Document and Benefit Fraud task forces in major U.S. cities, including Washington, D.C. There, as part of a continuing investigation known as Operation Card Shark, our agents have helped dismantle seven fraudulent document laboratories and secure convictions for 60 individuals to date.

As part of another task force led by State law enforcement officials, we also helped break up an extensive document mill operation run by MS-13 and other Latino gangs throughout New York City





and New Jersey. After months of undercover operations and surveillance, we arrested dozens of people, and seized thousands of fake Social Security cards.

As we delve deeper into these issues, we've found that many unauthorized workers have found a new way to slip through the cracks. In the past, they generally used fake documents containing invalid SSNs or SSNs that did not match the names on the documents. But now the trend is toward using entire identities of actual United States citizens.

Identity theft rings obtain personally identifiable information, and then sell documents containing these valid identities to unauthorized users. This new scheme has evolved as a way of circumventing employer verification services, which look for a match between the individual's name and SSN.

This is our newest employment-related challenge, because there's no way to identify this type of fraud unless the true number holder comes forward to report discrepancies in his or her earnings record. And because some of these number holders are children, we may not have that opportunity until they enter the workforce years from now.

Although detecting this fraud, and then investigating to a successful resolution, is difficult, we are making strides on audit and investigative fronts. For example, last September we released an audit assessing the validity of earnings posted

to the records of children ages 7 to 13. Although SSA flags earnings posted to records of children 6 or younger, this process does not cover ages 7 to 13.

We found that 88 percent of the earnings we reviewed did not appear to result from legitimate employment. Many of the employers were in industries that do not normally employ children, because they offer jobs not allowable for children under guidelines set by the Department of Labor.

SSA agreed with recommendations we made in that report, including that the Agency explore the idea of legislation to allow the disclosure of SSA information that may help other Federal agencies more effectively accomplish their missions. One such data-sharing effort already underway is the Department of Homeland Security's E-Verify program. Because SSA data is the foundation of this effort, we have been involved in evaluating and providing feedback.

In fact, last year, at the request of Congress, the OIG undertook three such evaluations, focusing on data accuracy and security. The first of these Congressional Response Reports, Accuracy of SSA's Numident File, has been oft-quoted by the media—and even more frequently mis-quoted.

In that study, we found errors in SSA's records that might result in what we call a "tentative non-confirmation" of an employee's work authorization. The media often cite that finding as evidence that E-Verify will cause innocent workers to be fired, and employers to be sued for discrimination.

Unfortunately, they're taking our findings out of context. Our auditors estimated that about 4 percent of all SSA's Numident records contained discrepancies in name, SSN, date of birth, or citizenship status that could result in a mismatch if submitted through E-Verify. What the media fail to mention is that our findings were based on a random sample of SSA's records, so many of those records belong to people whose SSNs were assigned decades ago. They are either deceased or retired, and would not

be applying for new jobs. Also ignored is the important fact that many of the errors are caused by individuals' failure to update their SSA

records when they get married or become legally authorized to work.

Of course, all Social Security numbers are vulnerable to misuse, but it's misleading to imply that using E-Verify will risk innocent employees' jobs. All employees would be given ample opportunity to correct their records with SSA before an employer could take any adverse action.

Nevertheless, we are fighting an uphill battle. No matter how many employers we arrest and how many audit reports we issue, we won't solve the problem of employment-related SSN misuse and discrepant earnings records until and unless we address our inability to share information among the various Federal agencies with a role in this process.

Rest assured that we will continue our audit work in these areas. We will continue our investigations, such as those I've described today. In particular, we will continue to pursue employers who knowingly provide false SSNs or documents to employees and false wage reports to SSA. And we will continue to work with SSA, Congress, and other agencies to make these efforts more effective.

I should note that all of the audit work I've mentioned today is available on our Web site, [www.socialsecurity.gov/oig](http://www.socialsecurity.gov/oig). The OIG, as an oversight body, will continue to do everything it can to ensure the integrity of the Social Security number. We will also encourage its protection by private and public entities; and provide meaningful sanctions for those who fail to protect it or who misuse it themselves.

Thanks once again to the Federal Bar Association for its efforts to foster a productive exchange on this issue of critical importance. I'm honored to have the opportunity to be here today, and I thank all of you for your interest and attention. ❧



# Patrick P. O'Carroll

**Patrick P. O'Carroll, Jr.** currently serves as the third Inspector General (IG) for the Social Security Administration, having been appointed to that position on November 24, 2004. Under his direction, the SSA Office of the Inspector General inspires public confidence in the integrity and security of SSA's programs by conducting independent and objective audits, evaluations, and investigations. Since assuming the SSA OIG leadership, Mr. O'Carroll has intensified the OIG's efforts to identify and prevent fraud, waste, and abuse in SSA programs through the institution of innovative and collaborative approaches to the office's core functions and the management and development of human and technological resources.

The results of these efforts can be seen in the OIG's most recent achievements. In FY 2008, the OIG's investigators reported over \$370 million in investigative accomplishments through SSA recoveries, restitution, fines, settlements, judgments, and projected savings. OIG auditors issued 108 reports with recommendations identifying over \$1.1 billion in federal funds that could be put to better use and \$2.4 billion in questioned costs. And OIG's attorneys reported over \$6.5 million in civil monetary penalties and assessments.

In addition to directing an OIG workforce of almost 600 auditors, attorneys, investigators, and support personnel nationwide, Mr. O'Carroll also chairs the Investigations Committee of the Council of the Inspectors General on Integrity and Efficiency, which addresses issues that transcend individual Government agencies, and increases the professionalism and effectiveness of IG personnel throughout the federal government. Under Mr. O'Carroll's leadership, the Committee has sought new ways to improve investigative functions, establish investigative guidelines, and promote best practices and training opportunities for thousands of agents in the federal IG community.

Prior to his appointment as Inspector General, Mr. O'Carroll held a number of increasingly responsible positions in the SSA OIG organization, including Assistant Inspector General for Investigations and Assistant Inspector General for External Affairs. Mr. O'Carroll also brought to the OIG the benefits of his 26 years of experience with the United States Secret Service.

Mr. O'Carroll received a B.S. from Mount Saint Mary's College in Emmitsburg, Maryland, and a Master of Forensic Sciences from the George Washington University, Washington, D.C. He also attended the National Cryptologic School and the Kennedy School at Harvard University. Mr. O'Carroll is a member of the International Association of Chiefs of Police and the Association of Government Accountants.