



SOCIAL SECURITY
Office of the Inspector General

June 26, 2012

The Honorable Charles Boustany
Chairman, Subcommittee on Oversight
Committee on Ways and Means
U.S. House of Representatives
B-317 Rayburn House Office Building
Washington, D.C. 20515

Attention: Kim Hildred

Dear Mr. Chairman:

This is in response to your June 15, 2012 correspondence asking questions for the record, further to my testimony on May 8, 2012 before the Subcommittees on Oversight and Social Security at a hearing on identity theft and tax fraud. I appreciate the opportunity to provide additional information regarding these critical issues. Below are responses to your specific questions.

1. The Social Security Administration has made the annual Social Security Statement available online, whereby a user must answer a series of questions to prove their identities. Are there any lessons the Internal Revenue Service could take from this, as it and other government agencies move to update their authentication techniques?

In May 2012, the Social Security Administration (SSA) implemented Electronic Access (EA) for its online statement, but has yet to expand EA to other Internet applications. Authentication through EA occurs completely online, eliminating the mailing of Password Request Codes for its PIN/Password applications. Although we have not audited SSA's EA protocols, we believe IRS can learn from SSA's experience—especially with respect to the lessons learned from the delays SSA experienced in attempting to make EA operational. We do know that the EA protocol uses multiple factors to authenticate users, which we believe is more effective than a single-factor authentication mechanism, such as a username and password.

In the 4th quarter of Fiscal Year 2012, we plan to initiate two audits related to SSA's EA and associated authentication. In the first review, *Security of the Social Security Administration's Public Facing Web Applications*, we will assess SSA's process to establish eAuthentication requirements for its public-facing web applications. Specifically, we will determine whether SSA's public-facing web application eAuthentication reasonably protects the confidentiality, availability, and integrity of the sensitive information used in the applications. Our contractor, Grant Thornton, LLP, will assess SSA's risk that an intruder could gain entry to the Agency's

Internet-accessible web application(s). To meet our objectives, the contractor will perform Web Application Penetration tests of SSA's sensitive and critical web applications, that will

- identify vulnerabilities within the information systems,
- determine opportunities that could be used to compromise the system or data,
- identify risks that could be reduced, and
- propose recommendations that could reduce opportunities to compromise the system based on weaknesses identified.

These tests will also assess the controls and security configurations in place to prevent a non-authorized individual from undermining the confidentiality, availability, or integrity of the sensitive information maintained at SSA.

Our second planned review, *The Social Security Administration's Public-facing Web Application Testing Process*, will assess whether (1) SSA's testing process for its public-facing web applications complies with Federal standards and best practices; and (2) implementation of or changes to public-facing web applications followed SSA's system-development life-cycle testing process. We will use any findings from our first review to identify where in the testing process the security weaknesses could have been prevented. Once these reviews are completed, we will have more definitive information on the effectiveness of the EA protocols.

2. Should State and local law enforcement have access to taxpayer information, such as refund date, in pursuing identity theft cases? Why or why not?

In cases involving Social Security number (SSN) misuse and identity theft, taxpayer information can be invaluable to law enforcement. Specifically, information regarding current and former employers, as well as past earnings reported under an SSN, might provide crucial investigative leads and evidence to support criminal charges of identity theft; to substantiate legitimate earnings versus illegal proceeds or concealment of work activity; or to assist law enforcement in locating a subject, fugitive, witness, or even a missing person.

The law enforcement community relies on assistance at all levels of government to conduct joint investigations of mutual interest and overlapping jurisdiction. Although currently we are able to share certain information contained within our case files with other law enforcement agencies during the course of joint investigations, we are prohibited from sharing "tax return" information, as the Internal Revenue Code strictly limits such disclosure. Pursuant to 26 U.S.C. § 6103, the OIG may disclose tax return information from its files only to the Department of Justice and if the disclosure is for the purpose of administering the *Social Security Act*. As such, the sharing of even basic tax return information, such as an individual's name, SSN, and employer, with our State/local law enforcement partners and prosecutors is restricted. We would support any exemption from these restrictions for law enforcement purposes.

3. Have you investigated any cases in which the Death Master File or a genealogical website was used to commit identity theft? In the last fiscal year, how many cases of Social Security number misuse cases did your office open?

Yes. In 2007, we participated in a joint investigation with IRS-Criminal Investigation regarding a fraudulent tax filing scheme. The investigation revealed that a Colorado man employed individuals so he could obtain names and SSNs of long-deceased individuals from a genealogical

website. The man then fabricated employment records and instructed others to use the obtained names, SSNs, and false employment information to create fraudulent tax returns, which were submitted to the IRS online. To determine deceased individuals' SSNs, the man said he compared data available from the public Internet site with a certain State's death data. The man was eventually convicted and sentenced to 46 months in prison for SSN misuse, making false claims, and wire fraud. He must also make restitution of over \$282,000 to the IRS.

Also, in August 2010, we began investigating about 60 fraudulent retirement benefit claims that used the name, SSN, and date of birth of individuals who died decades ago. We determined that the personally identifiable information (PII) used to file the fraudulent claims was available to the public through a genealogical website. The OIG and other law enforcement agencies identified suspects in the case and executed search and arrest warrants; however, the main suspect took his own life before he was taken into custody. His two accomplices, both relatives of his, were indicted and pled guilty to the charges. The two individuals received 20 months' and 25 months' in prison, respectively, and one was ordered to pay restitution of more than \$145,000 to SSA. In addition, they will be deported from the United States at the end of their sentences.

In Fiscal Year 2011, the OIG opened 286 cases involving SSN misuse, which accounted for approximately 3.9 percent of all cases opened during that period. We prioritize SSN misuse allegations that involve

- links to terrorist activities or other threats to national security,
- benefit fraud or other links to Social Security programs,
- Social Security employee misconduct, or
- counterfeiting or selling of Social Security cards.

4. I have submitted an article from a Florida newspaper for the record that reports that most fraudulent IRS refunds are made on prepaid debit cards. I am concerned that the government is moving to the debit card payment system, not only for tax refunds, but all government payments before adequate measures to prevent fraud are in place. Have you uncovered cases regarding debit card and other electronic payment systems where Social Security benefit payments are diverted to criminals? If so, are these also crimes of identity theft and how does that theft occur? How pervasive is this fraud?

We are currently investigating fraud involving the unauthorized diversion of Social Security benefits through the direct deposit process. Many of these scams involve the use of the Direct Express Debit MasterCard Program or some other type of reloadable pre-paid debit card account(s), as a means to redirect an individual's benefits without his or her knowledge and facilitate the movement of money.

There appear to be variations in how the fraud is being perpetrated against Social Security beneficiaries. These victims' PII may be compromised through some method of social engineering, or information may be acquired from those businesses or entities with access to PII, such as financial services, health care-providers, etc.

Our investigations confirm that this appears to be a "cottage industry" scam. The majority of our victims are elderly beneficiaries, and they are geographically dispersed throughout the country. We estimate there are thousands of victims, consisting of individuals who have either had their

benefits fraudulently redirected, or an attempt was made to redirect their benefits. Regardless, all these individuals appear to be victims of identity theft.

5. What action should be taken to prevent debit card fraud?

Our investigations disclose that fraud involving pre-paid debit cards can be perpetrated anonymously and remotely, potentially minimizing a subject's risk of being caught. Reloadable pre-paid debit cards raise concerns because there are limited controls to authenticate the cardholder. Individuals can simply purchase these cards online or through a local retailer; and after providing the necessary information, can receive direct deposit payments onto the card.

We would encourage examining the strength of existing authentication procedures for the auto-enrollment process established between the Department of Treasury, financial institutions, and those government agencies charged with the responsibility of administering Federal benefit programs. We would also encourage agencies to review their authentication and verification methods for altering payment information.

Thank you for the opportunity to clarify these issues for the Subcommittees on Oversight and Social Security. I trust that I have been responsive to your request. I have sent a similar letter to Chairman Johnson.

If you have further questions, please feel free to contact me, or your staff may contact Misha Kelly, Special Agent-in-Charge of Congressional Affairs, at (202) 358-6319.

Sincerely,

A handwritten signature in blue ink, appearing to read "Patrick P. O'Carroll, Jr.", written in a cursive style.

Patrick P. O'Carroll, Jr.
Inspector General