# U.S. House of Representatives

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

**Statement for the Record**

**Hearing on the Direct Deposit of Social Security Benefits**

**The Honorable Patrick P. O'Carroll, Jr.**
**Inspector General, Social Security Administration**

**September 12, 2012**

Good morning, Chairman Johnson, Ranking Member Becerra, and members of the Subcommittee. It is a pleasure to appear before you, and I thank you for the invitation to testify today. I have appeared before Congress many times to discuss issues critical to the Social Security Administration (SSA) and the services the Agency provides. Today, we are addressing a current and serious challenge for the Agency and its beneficiaries: identity thieves' fraudulent redirection of Social Security benefit payments.

**Background**

SSA certifies payments to Social Security beneficiaries; this certification effectively authorizes the release of such payments.[1] In response, Department of the Treasury issues the payment, by paper check or some form of direct deposit. Ninety-four percent of Social Security benefit payments and 82 percent of SSI payments are made through direct deposit. Beneficiaries who enroll in direct deposit can receive payments through:

- traditional financial institutions, including electronic-transfer accounts,
- the Treasury's Direct Express Debit MasterCard Program, or
- various pre-paid debit cards.

Pursuant to a Federal regulation, on March 1, 2013, the Treasury will require almost all beneficiaries to receive payments through direct deposit, though paper checks will still be available to some beneficiaries under very limited circumstances. SSA thus expects an increase in direct deposit-related enrollments from its customers. Direct deposit payments offer a timely, convenient, and secure method for people to receive their federal benefits, instead of cashing a paper check; the Treasury has also stated the move to electronic benefit payments would cut costs associated with issuing paper checks. We fully support SSA's and the Treasury's efforts to make this transition. Nevertheless, we are concerned that some beneficiaries who have become victims of identity theft have found that the criminals responsible used their personally identifiable information to redirect their Social Security benefits to another financial account without their authorization.

SSA offers beneficiaries several ways to make changes to direct deposit information: in person at an SSA field office, over the phone, via the Internet, or through the beneficiary's financial institution. In October 2011, the SSA Office of the Inspector General (OIG) began tracking allegations indicating that individuals—other than the Social Security beneficiaries or their representative payees—had initiated potentially unauthorized changes to direct deposit information and redirected beneficiary payments to other accounts. As of August 31, 2012, my office has received more than 19,000 reports from various sources concerning questionable direct deposit changes to a beneficiary's record; we continue to receive about 50 such reports per day. These reports have involved either an unauthorized change to direct deposit information, or a suspected attempt to make such a change.

**OIG Response**

[1] The term "beneficiary" refers to both Social Security beneficiaries and Supplement Security Income recipients.

My office has responded to these reports by opening multiple investigations across the country. Thus far, we have determined the suspects have predominantly targeted older citizens' personally identifiable information (PII) through various methods of social engineering, such as telemarketing and lottery schemes, as well as through other sources. After obtaining the PII, the suspects have used the information to initiate a direct deposit change and redirect a victim's benefits to a fraudulent account.

We continue to encounter beneficiaries who have been victimized and severely affected by this scheme. For example, in August 2011, an 86-year-old beneficiary received a letter indicating he won $3.5 million. The letter included a phone number and requested he provide some personal information so that he could collect his winnings; the man called the number and submitted some of his information.

Within days of the phone call, an unauthorized change was made to the man's direct deposit information with SSA. Soon after, the man did not receive his scheduled Social Security payment, so he contacted SSA, only to learn that his benefits were diverted to a different account. He was issued a replacement payment, but the man reported that the ordeal caused two months of hardship, as he was forced to obtain a bank loan to pay his rent and for other living expenses. Additionally, our audit work determined the man's payments were diverted a second time; he was again issued a replacement payment.

In another unsettling example, a 68-year-old beneficiary's direct deposit information was changed 13 times in an eight-month period, according to SSA's records. In this case, an individual called the man and claimed to be an official from a well-known sweepstakes company; he said the man won $2.5 million, but the man needed to send money to the caller to receive all of his winnings.

The beneficiary reported that he sent several thousand dollars to the caller through a financial service company. He also reportedly sent $1,000 to the caller through two pre-paid debit cards. The beneficiary provided his personal information to the caller during these transactions, and subsequently, his direct deposit information was changed multiple times over the next several months, with his benefit payments redirected to at least six different pre-paid debit cards during that time. Unauthorized account changes occurred several times throughout a payment cycle in an attempt to redirect his benefits.

The threat of identity theft and misuse of Government funds is evident, as unscrupulous individuals continue to target some of our most vulnerable citizens. My office has partnered with the Treasury OIG to investigate these schemes, some of which have roots in Jamaica but reach across the United States. Our special agents are also working with other Federal law enforcement agencies, such as the U.S. Postal Inspection Service and Immigration and Customs Enforcement, in ongoing investigations.

As part of our investigative efforts, our special agents, along with Treasury OIG, traveled to Jamaica in June 2012, and met with U.S. officials regarding this matter. Our investigators continue to share information with U.S. law enforcement from the embassy in Jamaica.

We are working with U.S. Attorneys Offices across the country, and State and local prosecutors, to bring charges against individuals perpetrating this fraud. We have executed search warrants, made arrests, and worked with prosecutors to charge several individuals.

For example:

- A U.S. citizen and a Jamaican National residing in St. Louis pleaded guilty to Federal charges including identity theft and wire fraud. They reportedly targeted beneficiaries throughout the country, deceiving the beneficiaries into sending them money through wire transfers and pre-paid debit cards. The individuals allegedly sent the beneficiaries' money to another Jamaican National in Montego Bay, Jamaica. The suspect in Jamaica faces similar charges, but has not been arrested.

- In Florida, our special agents investigated several individuals who allegedly stole victims' PII and redirected tax refund checks and Social Security benefits to pre-paid debit cards. Two individuals were charged with identity theft and conspiracy to commit wire fraud and mail fraud.

- In New York, our special agents arrested a man who reportedly stole beneficiaries' PII and redirected their payments to pre-paid debit cards. He reportedly used the cards to make ATM withdrawals and pay for store purchases. He faces charges of identity theft and grand larceny.

**Reviews and Recommendations**

While investigating this fraudulent scheme on several fronts, we also initiated several reviews of SSA's controls over the processing of beneficiary direct deposit information.

I mentioned that SSA offers beneficiaries several ways to change their personal and financial records; one of those ways is by calling the Agency's national 800-phone number, where trained SSA staff can process requests to initiate, change, or cancel a direct deposit plan.

As reports of attempts to make unauthorized changes to beneficiary accounts surfaced, SSA in November 2011 revised its policy for verifying the identities of individuals who request direct deposit changes over the phone. The Agency also reminded staff how to properly process such requests over the phone, especially if notations in SSA systems indicated a beneficiary's information was previously changed fraudulently.

Despite this, our review of the Agency's controls over direct deposit routing-number changes by phone found that they were not fully effective. Accurately verifying an individual's identity over the phone presents more challenges to SSA staff than a face-to-face verification in a field office; thus, the risk of fraudulent record changes increases when staff processes requests over the phone.

SSA needs sufficient authentication controls in place to prevent the processing of potentially unauthorized changes to a beneficiary's direct deposit records. Confirming a beneficiary's PII does not guarantee the caller is the beneficiary; SSA has beneficiary-specific information in its systems it could request for additional verification purposes.

In another review, we have found that the Agency's controls over direct deposit account changes made in SSA field offices were not fully effective. We found that SSA's procedures to redirect Social Security payments required a *lower level* of identity verification than for other business transactions. SSA should implement more robust identity verification procedures before processing account changes.

Beneficiaries may also make direct deposit changes through automated enrollment with financial institutions; in Calendar Year 2011, this method accounted for a large number of account changes, including initiating direct deposit. The financial institutions then forward the account information to SSA through the Treasury. However, we found several financial institutions provided SSA unauthorized direct deposit changes through automated enrollment requests, which the Agency then processed. SSA has stated its systems are not designed to prevent processing unauthorized automated enrollment changes. Moreover, financial institutions perform identity verification at their own discretion; they themselves must implement reasonable procedures to verify the identities of individuals who open new accounts. Because SSA relies on the financial community for accurate and secure information, but is not directly involved with the individual institutions, the Agency must work with the Treasury to improve banks and credit unions' identity verification controls for account changes.

In addition to what appeared to be unauthorized direct deposit changes using traditional bank accounts, we found that some financial institutions provided potentially fraudulent direct deposit changes to prepaid debit cards. Beneficiaries can use any of SSA's direct deposit change methods to redirect their benefits to a prepaid debit card. These cards are purchased at retailers or online. Financial institutions issue these cards through many different service providers. In August, a major pre-paid debit card vendor informed my office that it would add additional authentication controls to its online Federal-payment enrollment process by the end of the year. The Treasury should also consider the option of developing unique routing numbers for pre-paid debit cards, as these cards are particularly tempting tools for benefit thieves.

We have also reviewed the Treasury's Direct Express debit card program. Direct Express is a low-cost program, administered by Comerica Bank, which allows beneficiaries who do not have a bank account to access their Federal benefit payments with a debit card.

We found that SSA could improve its controls over the enrollment and post-entitlement process for beneficiaries in the Direct Express program. When Comerica initiates and verifies identification for Direct Express enrollments with SSA, the Agency matches a limited amount of beneficiary information against the Direct Express record to verify and approve the enrollment. SSA should work with the Treasury and Comerica to enhance identity verification for enrollment and incorporate SSA policies into the Direct Express program. For example, Direct Express should not allow multiple beneficiaries to enroll on the same card without SSA's explicit approval; and debit cards should not be sent to foreign addresses if residency is a factor in continuing eligibility for benefits, as in the Supplemental Security Income program.

We are working on one additional report that will quantify the cost of replacing Social Security benefit payments that were lost due to unauthorized direct deposit changes.

**Suggested Controls over Account Changes**

We have done and continue to do significant audit work on this issue, but there are several controls the Agency could implement quickly to reduce fraudulent direct deposit changes:

1. Continue the planned implementation to block auto-enrollments for individuals who express concerns about fraudulent attempts to change their direct deposit information through auto-enrollment. SSA has reported to us they plan to implement an auto enrollment "block" in October 2012 .

2. Develop an automated notification system to alert beneficiaries of changes made to their direct deposit information; for example, through an automatic e-mail, a text message, or a notice mailed to both the old and new addresses on record when a caller requests and SSA processes an address and direct deposit change at the same time.

3. Consider delaying direct deposit changes for a certain amount of time, instead of implementing changes immediately after receiving a request for a change, to identify potential overpayments before they are made.

Additionally, my office continues to urge all individuals, especially older beneficiaries, to take basic preventive steps to protect their personal information from improper use. We urge everyone to be aware of the prevalence of phishing and lottery schemes—no reputable financial institution or company will ask for upfront money in exchange for additional winnings; or for personal information like a Social Security number or bank account number via phone, mail, or Internet. Moreover, when Social Security beneficiaries become aware that they are victims of identity theft, they can block electronic access to their information in SSA's records, a service available at www.socialsecurity.gov/blockaccess. By knowing how to protect ourselves, we make life much more difficult for identity thieves.

**Conclusion**

My office has responded to this widespread fraud scheme with multiple investigations across the country and collaborations with other government and law enforcement agencies. We have initiated a variety of audit reviews with several policy and authentication recommendations to SSA, the Treasury, and financial institutions. We have also increased our public outreach efforts, producing a YouTube public service announcement on protecting personal information, and publishing several OIG website articles and blog posts about fraudulent lottery schemes and guarding against identity theft.

The recent rash of fraudulent changes to Social Security beneficiary accounts is a serious issue facing SSA, and the Agency must act swiftly to protect beneficiaries and taxpayer dollars. As almost all Social Security beneficiaries will soon receive their payments electronically, SSA must quickly implement policy changes and work with the Treasury, which has oversight of the financial community, to guard against identity thieves who will continue their attempts to defraud SSA and its beneficiaries.

We will continue to provide information to your Subcommittee and Agency decision-makers as we address this issue. Thank you again for the opportunity to speak with you today. I am happy to answer any questions.