United States Senate

Special Committee on Aging

Statement for the Record

Social Security Payments Go Paperless: Protecting Seniors from Fraud and Confusion

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

June 19, 2013

Good afternoon, Chairman Nelson, Ranking Member Collins, and members of the Committee. It is a pleasure to appear before you, and I thank you for the invitation to testify. Today, we are discussing the Social Security Administration's (SSA) transition to electronic payments and related concerns, including identity thieves' fraudulent redirection of Social Security benefits.

Background

SSA certifies payments to Social Security beneficiaries; this certification effectively authorizes the release of such payments.[1] In response, the Department of the Treasury issues the payment. Pursuant to a new Federal regulation, as of March 1, 2013, the Treasury required almost all beneficiaries to receive payments through direct deposit, though paper checks are still available to some beneficiaries under limited circumstances. Beneficiaries enrolled in direct deposit can receive payments through:

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

SSA certifies payments for more than 60 million people each month. 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 will cut costs associated with issuing paper checks. In the lead up to this transition, we have fully supported SSA's and the Treasury's efforts.

However, we remain concerned that some beneficiaries who become victims of identity theft will find that their monthly Social Security benefits have been redirected, sometimes repeatedly, to another financial account without their authorization.

SSA offers beneficiaries several ways to make changes to direct deposit information: online, in person at a local Social Security office, over the phone, 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 benefit payments to other accounts. As of June 1, 2013, my office has received more than 37,000 reports from various sources concerning questionable 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; these changes predominantly involve redirecting benefits to prepaid debit card accounts. Thus far, we have determined the suspects have targeted and obtained senior citizens' personally identifiable information through various methods of social engineering, such as telemarketing and lottery schemes, or through other sources.

Moreover, my office recently began receiving reports of direct deposit fraud committed through SSA's *my Social Security* online portal. SSA expanded *my Social Security* in January 2013, allowing beneficiaries not only to view their earnings record and benefit estimates, but also to change their address of record and direct deposit information. Since then, SSA reports that more than 22,000 potentially fraudulent *my Social Security* accounts have been opened. It appears that many of these fraudulent *my Social Security* accounts were established to redirect Social Security benefits to

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

unauthorized bank accounts. The OIG has received—from SSA and other sources—more than 6,200 fraud allegations related to *my Social Security*, but it is important to note that each of these allegations may involve multiple fraudulent *my Social Security* accounts.

We continue to encounter beneficiaries who have been victimized and severely affected by these schemes. For example, in 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 his information.

Within days of the phone call, an unauthorized change was made to the man's Social Security direct deposit information. Soon after, the man did not receive his scheduled benefit payment, so he contacted SSA, only to learn that his benefits were diverted to another 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.

In another unsettling example, Social Security benefits were redirected to a woman's bank account through a fraudulent *my Social Security* account. The woman said she received a phone call in March from a caller who said she won $1.5 million. The caller instructed the woman to open a bank account so that she could receive funds to pay for "taxes" on the winnings; she was then instructed to withdraw the funds from the account and place them on prepaid debit cards. The woman then provided the debit card numbers to a suspect over the phone. She also said, around that time, she and her husband received letters from SSA indicating they had established *my Social Security* accounts, when in fact, they had not.

OIG Response

We have responded to these reports by opening multiple investigations across the country. I am pleased to report that earlier this month, a major organizer of one of these fraud schemes pled guilty in Wisconsin to defrauding hundreds of thousands of dollars from vulnerable seniors across the country. O'Brain J. Lynch, 28, of Jamaica, pled guilty to wire fraud and faces a maximum of 20 years in prison. As part of his plea agreement, he has agreed to pay at least $100,000 in restitution.

Lynch and his co-conspirators reportedly developed an extensive Jamaican lottery scheme to identify victims, deceive them to obtain personal information, and use that information to change their address record and redirect their benefits to a third party, who wired the stolen money to Jamaica. They also used victims' money to order items in the United States like jewelry, cell phones, tablets, and other electronics, before sending the items to Jamaica to keep them from being traced.

OIG special agents worked closely with the U.S. Postal Inspection Service (USPIS) and Homeland Security Investigations to identify Lynch and arrest him in in North Carolina in February. Lynch's arrest and subsequent plea represents a significant breakthrough in the ongoing investigation of these schemes.

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

For example:

- In November 2012, as part of an OIG investigation, two Florida women were sentenced for their roles in a scheme to fraudulently redirect Social Security benefits to prepaid debit card accounts, including Direct Express accounts. After pleading guilty to identity theft and mail and wire fraud, the women were sentenced to 51 months and 45 months in prison, respectively.

- In October 2012, as part of an OIG investigation, two individuals residing in St. Louis were sentenced to 3 years' probation and ordered to pay more than $38,000 to various victims, after pleading guilty to identity theft and wire fraud. The individuals reportedly targeted beneficiaries throughout the country, deceiving the beneficiaries into sending them money through wire transfers and prepaid debit cards. They reportedly sent the beneficiaries' money to another Jamaican National in Montego Bay, Jamaica, who remains a fugitive.

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. Also, in December 2012, our agents attended a USPIS-sponsored Jamaican Operations Linked to Telemarketing (JOLT) task force meeting, joining representatives from other law enforcement agencies, the Jamaican government, and private businesses. Our investigators continue to share information with our law enforcement partners.

Reviews and Recommendations

While investigating these fraudulent schemes on several fronts, we have completed and we continue to perform significant audit work related to these issues. Our most recent review, still in progress, seeks to quantify the cost of replacing missing Social Security benefit payments due to unauthorized direct deposit changes. Our auditors identified more than 23,000 beneficiaries who reported they did not receive about 25,700 Social Security payments worth about $28.3 million between September 2011 and June 2012. We further found that:

- SSA recovered $10.9 million, but it did not recover about $17.4 million of the reported missing payments.

- SSA sent about $17.4 million in replacement payments to beneficiaries, including $6.7 million to beneficiaries whose initial missing payments were never recovered.

- SSA did not replace $10.9 million of reported missing payments; but the Agency may be responsible to replace these payments. SSA recovered $200,000 of these initial payments, so the Agency will have an additional loss of $10.7 million if all missing payments are replaced.

For the nine-month period of our review, SSA faces a potential loss of $17.4 million because of missing benefit payments due to possible unauthorized direct deposit changes that have not been recovered. We plan to issue this report by August.

As I mentioned, many of these fraudulent direct deposit changes involve redirecting benefits to prepaid debit cards, which financial institutions offer at retailers or online. The changes are made with the financial institution, which forwards the account information to SSA through the Treasury. In another review, we found that some financial institutions provided the Treasury potentially fraudulent direct deposit changes to prepaid debit cards. Last year, a major prepaid debit card vendor informed my office that it would add other authentication controls to its online Federal-payment enrollment process. The

Treasury should also consider the option of developing unique routing numbers for prepaid 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. About 3.2 million beneficiaries are currently enrolled in the Direct Express program.

We found SSA could improve its controls over the processing beneficiary transactions 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.
In the last year, we have also issued audit reports that reviewed controls over direct deposit changes initiated by the Agency's national 800-phone number, in local Social Security offices, and through SSA's online applications. In several instances, we found that controls in place were not fully effective, and authentication methods could be improved.

The Agency has taken the following steps to strengthen controls over changes to direct deposit information:

- SSA has revised its policy for verifying callers who request direct deposit changes, and it issued reminders to staff to properly process callers' requests for direct deposit changes, especially if the beneficiary record indicates information was previously changed fraudulently.
- In November 2012, SSA implemented the Direct Deposit Auto-Enrollment[2] Fraud Prevention tool, which allows beneficiaries to request that direct deposit changes made through auto-enrollment are blocked.
- In March 2013, SSA terminated Direct Deposit Automated Applications for field-office callers and 800-number callers.
- SSA has assembled a task force to address access changes needed for the *my Social Security* application; the Agency has installed temporary authentication controls on *my Social Security* to improve security; and it will continue to review online security measures.

Suggested Controls over Account Changes

There are several other controls SSA could implement quickly to reduce fraudulent direct deposit changes:

[2] Auto Enrollment is the process by which a financial institution may send enrollment information through the Automated Clearing House (ACH) directly to SSA.

1. Work with the Treasury to enhance identity verification processes for direct deposit changes initiated by financial institutions, to prevent the fraudulent redirection of benefits to prepaid debit cards.

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. Delay 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 winnings; or for personal information like a Social Security number or bank account number via phone, mail, or the Internet. If Social Security beneficiaries do become victims of identity theft, they can block electronic access to their information in SSA's records, a service available at www.socialsecurity.gov/blockaccess. Finally, all individuals can prevent someone from establishing a fraudulent *my Social Security* account in their name by establishing a legitimate account themselves at www.socialsecurity.gov/myaccount. 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, highlighted by the recent arrest and guilty plea of O'Brain J. Lynch. We have completed 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 fraud advisories and blog posts about fraudulent lottery schemes and guarding against identity theft.

The growing incidence of fraudulent changes to Social Security beneficiary accounts and *my Social Security* information is a serious issue facing SSA; the Agency must act swiftly to protect beneficiaries and taxpayer dollars, as nearly all Social Security beneficiaries now receive payments through direct deposit. SSA should continue to 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 Committee 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.