



Social Security Administration
Office of the Inspector General

Direct Deposit Changes Initiated Through Financial Institutions and the Social Security Administration's Internet and Automated 800-Number Applications (Limited Distribution) **(A-14-12-21271)**

Our objective was to determine the effectiveness of controls over direct deposit changes originating in financial institutions (FI), including prepaid debit cards. We expanded the scope of our review to include a determination of the effectiveness of controls over direct deposit changes originating through the Social Security Administration's (SSA) Direct Deposit Internet and automated 800-number applications.

BACKGROUND

SSA encourages beneficiaries to use direct deposit for their benefit payments. The Agency makes approximately 95 percent of Title II Social Security payments and 85 percent of Title XVI Supplemental Security Income payments through direct deposit to FIs. Pursuant to recent changes in Federal regulation, beginning March 1, 2013, beneficiaries will be required to receive their payments through direct deposit unless they qualify for a waiver. The Agency anticipates that the volume of direct deposit-related requests from beneficiaries will increase as a result of this change.

SSA offers its customers a variety of methods to initiate a direct deposit change. For this report, we reviewed direct deposit changes made through FIs and SSA's Direct Deposit Internet and automated 800-number applications. We also reviewed direct deposit changes made to prepaid debit cards. These cards are purchased at retailers or online. FIs issue these cards through many different service providers. Like traditional bank accounts, prepaid debit cards have routing and account numbers. Therefore, beneficiaries can use any of SSA's direct deposit change methods to redirect their benefits to a prepaid debit card.

Beneficiaries can request that FIs send their direct deposit information to SSA through the Department of the Treasury. To direct SSA benefits to an existing checking or savings account, FIs use an electronic process known as Automated Enrollment. FIs that choose to participate in this process are responsible for verifying the requesters' identities.

Title II beneficiaries can use SSA's Direct Deposit Internet application on the Agency's Website to change direct deposit account information. To use this application, a beneficiary must log in through SSA's personal identification number (PIN)/password authentication, using their Social Security number as their PIN. Title II beneficiaries can also call SSA's automated 800-number application to initiate or change direct deposit information. This application uses advanced speech recognition technology to change a beneficiary's account information. To confirm beneficiaries are who they claim to be, the Agency authenticates them using either knowledge-based authentication or the PIN/password methodology described above.

SSA has taken efforts to prevent fraudulent direct deposit changes. On February 17, 2012, SSA revised its policy for verifying the identity of callers who request to establish, change, or cancel direct deposit payments. In addition, SSA issued reminders to its staff on how to properly process callers' requests to change direct deposit information. On May 7, 2012, the Agency provided interim guidance for handling direct deposit fraud allegations. Further, SSA representatives stated that the Agency has various projects underway that would improve controls over direct deposit changes.

In October 2011, we began tracking allegations that indicated individuals other than the beneficiaries or their representatives had redirected benefit payments from the beneficiaries' bank accounts to accounts the individuals controlled. As of August 31, 2012, we had received over 19,000 reports concerning direct deposit changes to an SSA beneficiary's record. These reports involved either an unauthorized change or a suspected attempt to make an unauthorized change. Based on these allegations, we initiated audits to evaluate controls in the direct deposit process and identify vulnerabilities.

To determine the effectiveness of SSA's controls over changes to direct deposit information initiated through FIs or the Agency's Direct Deposit Internet or automated 800-number applications, we reviewed SSA's policies and procedures on direct deposit changes as well as SSA systems documentation. We also identified suspicious direct deposit changes that were initiated through FIs or SSA's Direct Deposit Internet or automated 800-number applications in September or October 2011 followed by a report of a non-receipt of payment, followed by another direct deposit change for the same beneficiaries. We then selected a sample of 40 beneficiaries to interview.

RESULTS OF REVIEW

Our interviews with beneficiaries confirmed that FIs provided SSA with unauthorized direct deposit changes, which the Agency processed. We also found SSA had some controls to prevent unauthorized direct deposit changes originating through the Agency's Direct Deposit Internet and automated 800-number applications. However, we identified weaknesses in SSA's authentication process for these applications. Based on our review, we do not believe SSA had adequate controls in place to prevent processing or alert Agency staff of potentially unauthorized changes to a beneficiary's direct deposit information.

SSA has improved controls over changing direct deposit information. However, more needs to be done to reduce the risk of processing unauthorized account changes. Throughout our report, we identify opportunities for the Agency to implement controls to help prevent the fraudulent redirection of benefits.

From our population of suspicious direct deposit changes, we selected a sample of 40 beneficiaries to interview. We only interviewed 35 of the 40 beneficiaries selected because 2 beneficiaries did not respond to our attempts to contact them, 1 refused to meet with us, and 2 were very ill. For the 35 interviews conducted, 6 beneficiaries reported they had authorized the direct deposit changes, and 29 reported they had not. The six beneficiaries who authorized the changes reported a non-receipt of benefits because they forgot about the change or because of confusion after switching banks or moving into a health care facility. When we asked the 29 beneficiaries who did not authorize the direct deposit changes how someone might have gained access to their private information to make a change, the results were as follows.

- Thirteen beneficiaries reported they were told they had won a lottery, but they needed to provide some private information before they could receive their prize.

- Three beneficiaries said they provided their private information to someone claiming to be an official from a Government agency or someone they knew.
- Two beneficiaries reported their wallets or credit cards had been lost or stolen.
- Eleven beneficiaries reported they were unsure how someone might have acquired their private information.

Of the 29 beneficiaries in our sample with misdirected benefit payments, the suspicious direct deposit changes for 19 beneficiaries originated at FIs, for 9 beneficiaries the direct deposit change originated through SSA's Direct Deposit automated 800-number application with knowledge-based authentication, and for 1 beneficiary the direct deposit change originated through the Agency's Direct Deposit Internet application. For the 19 beneficiaries with changes originating at FIs, we determined that changes for 9 beneficiaries redirected benefits to prepaid debit cards. The changes for the remaining 10 beneficiaries redirected benefits to accounts we could not identify as prepaid debit cards.

The 29 beneficiaries reported to SSA that they did not receive 51 benefit payments, totaling \$62,639, between September 1, 2011 and April 30, 2012. Of the \$62,639, we identified \$43,405 in replacement payments made to the beneficiaries as of April 30, 2012. The Agency made these replacement payments to 23 (79 percent) of the 29 beneficiaries representing 35 (69 percent) of the 51 non-receipts. Of the 35 non-receipts for which we identified replacement payments, the replacement payments for 25 (71 percent) were made within 30 days of the non-receipt being recorded. We also determined that as of April 30, 2012, SSA had recovered from FIs \$19,614 of the \$62,639 reported as non-receipts (31 percent).

We also determined SSA assessed overpayments, totaling \$12,571, to 8 of the 29 beneficiaries. For example, one beneficiary we interviewed reported that he did not receive his October 2011 benefit, and the Agency issued a critical payment as reimbursement. However, the beneficiary received a notice indicating that SSA had paid his October 2011 benefits twice. Of the \$12,571 in overpayments assessed, SSA collected \$1,533 from the beneficiaries and waived or deleted \$1,956. The remaining \$9,082 was still outstanding on the beneficiaries' records as of April 30, 2012 and may or may not be collected. After discussing the above overpayment issue with SSA, the Agency released a temporary policy instruction that directed SSA employees to suppress overpayment notices and stop recovery efforts when direct deposit fraud is alleged.

CONCLUSION

We determined that the controls over direct deposit changes originating through FIs or the Agency's Direct Deposit Internet and automated 800-number applications did not ensure all changes were authorized. Based on beneficiary interviews, data analysis, and our review of systems documentation, we identified instances of unauthorized account changes and weaknesses in SSA and FI's authentication or identity verification processes.

Although SSA cannot prevent beneficiaries from providing personally identifiable information to fraudsters, there are opportunities for the Agency to improve its control over direct deposit changes and reduce the risk of making benefit payments to unauthorized accounts. Moreover, some of the improvements we recommend apply Agencywide, regardless of how someone initiates a direct deposit change. We made nine recommendations. SSA agreed with eight of our nine recommendations.

This report contains restricted information for official use. Distribution is limited to authorized officials.