Verifying the Identities of Individuals Who File Internet Claims
A-14-18-50640

SOCIAL SECURITY
ADMINISTRATION
OIG

Objective

To answer congressional questions about the Social Security Administration's (SSA) Internet Claims system (iClaim).

Background

SSA's iClaim allows individuals to establish claims online for retirement, Medicare, spousal, and disability insurance benefits.

On February 28, 2018, Chairman Johnson and Ranking Member Larson, Subcommittee on Social Security, requested that we answer the following questions: (1) How has SSA improved its ability to authenticate iClaim applications since the OIG's 2011 audit? (2) How many fraudulent iClaim applications were identified each year in 2011 through 2017? How many of them were identified before payments were issued, and how many after? How did SSA determine that such claims were fraudulent? (3) What is the total value of payments paid on these fraudulent iClaim applications each year in 2011 through 2017? (4) What is SSA's plan for reviewing the security of iClaim, assessing its vulnerability to fraudulent applications, and mitigating these risks? (5) What is your assessment of this plan? Do you have additional recommendations?

Conclusions

SSA had not changed its authentication process for the iClaim application until September 29, 2018, when the Agency implemented new controls to help ensure individuals who submit iClaim applications are who they claim to be. Since 2016, SSA has used a predictive model to identify potentially fraudulent benefit claims for further review. SSA began tracking potential and likely fraudulent iClaim applications in late summer 2014. In Fiscal Year (FY) 2015, SSA identified 89 likely fraudulent iClaim applications. In FY 2018, that number increased to 62,794. The Agency does not track whether it issued payments before it identified claims as likely fraudulent.

Over the last several years, SSA has primarily focused on implementing controls designed to detect—after individuals submitted iClaim applications—whether those applications were potentially fraudulent. On September 29, 2018, the Agency began using the same identity-proofing controls for iClaim that it uses for its *my* Social Security portal. While SSA expects this will help prevent individuals from submitting fraudulent iClaim applications, our prior audits have identified concerns with the portal's security. Because the Agency's controls for the *my* Social Security portal have not prevented all individuals from fraudulently establishing accounts or submitting direct deposit transactions, using those same controls for iClaim may not prevent all individuals from fraudulently submitting iClaim applications.

SSA needs to implement controls to fully address Federal identity requirements and ensure individuals using its online services—including iClaim—are who they claim to be.

In response to our draft report, SSA indicated it is continually reviewing its systems to ensure it identifies potential fraud risks, document existing controls, and determine whether additional controls are necessary. According to the Agency, an important part of its strategy is establishing an authentication process that
(1) integrates the new Federal guidelines for digital identities;
(2) meets the ever-changing cyber-threat landscape; and
(3) balances ease of use for customers with a strong level of privacy and security.