



SOCIAL SECURITY ADMINISTRATION

[Docket No. SSA-2018-0012]

Privacy Act of 1974; System of Records

AGENCY: Office of Analytics, Review, and Oversight, Social Security Administration (SSA).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act, we are issuing public notice of our intent to modify an existing system of records entitled, Anti-Fraud Enterprise Solution (AFES) (60-0388), last published on May 3, 2018. This notice publishes details of the modified system as set forth under the caption, SUPPLEMENTARY INFORMATION.

DATES: The system of records notice (SORN) is applicable upon its publication in today's Federal Register. We invite public comment on the routine uses or other aspects of this SORN. In accordance with 5 U.S.C. 552a(e)(4) and (e)(11), the public is given a 30-day period in which to submit comments. Therefore, please submit any comments by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: The public, Office of Management and Budget (OMB), and Congress may comment on this publication by writing to the Executive Director, Office of Privacy and Disclosure, Office of the General Counsel, SSA, Room G-401 West High Rise, 6401 Security Boulevard, Baltimore, Maryland 21235-6401, or through the Federal e-Rulemaking Portal at <http://www.regulations.gov>. Please reference docket number SSA-2018-0012. All comments we receive will be available for public inspection at the above address and we will post them to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Neil Etter, Government Information Specialist, Privacy Implementation Division, Office of Privacy and Disclosure, Office of

the General Counsel, SSA, Room G-401 West High Rise, 6401 Security Boulevard,
Baltimore, Maryland 21235-6401, telephone: (410) 966-5855, email:
Neil.Etter@ssa.gov.

SUPPLEMENTARY INFORMATION: We are modifying the system of records name from “Anti-Fraud Enterprise Solution” to “Anti-Fraud (AF) System” to reflect the system accurately. The AF System is an agency-wide and overarching system that we use to detect, prevent, and mitigate fraud in SSA’s programs. The AF System collects and maintains personally identifiable information (PII) to assist in identifying suspicious or potentially fraudulent activities performed by individuals across our programs and service delivery methods.

We are claiming that the AF System is exempt from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Some information in the AF System relates to our efforts to mitigate, detect, and investigate fraud in Social Security’s programs and systems and to collaborate with the Office of the Inspector General in fraud investigations and prosecutions. Therefore, we need these exemptions to protect information from public access. The exemptions are required to avoid disclosure of screening techniques; to protect the identities and physical safety of confidential informants; to ensure our ability to obtain information from third parties and other sources; and to protect the privacy of third parties. Allowing an individual to access the information in AF System could permit the individual to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of the AF System and the overall law enforcement process, we may, at our discretion, grant notification of or access to a record in the AF System. If an individual is denied any right, privilege, or benefit to which he or she is otherwise entitled under Federal law due to the maintenance of material in the AF System, we will provide such material to such individual, except to the extent that the

disclosure of such material would reveal the identity of a source who furnished information to us under an express promise that the identity of the source would be held in confidence.

SSA claims exemption from Privacy Act subsection (c)(3) (Accounting and Disclosure); subsection (d) (Access and Amendment to Records); subsection (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements); and subsection (f) (Agency Rules) for this system of records. We claim exemption from these Privacy Act subsections for the AF System because release of the accounting of disclosures, access to the records, and notice to individuals with respect to existence of records could alert the individual whom might be a subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation. Disclosures of accounting would therefore present a serious impediment to law enforcement efforts. These Privacy Act subsections would permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses, or evidence, and to avoid detection or apprehension, which would undermine the investigative process. Thereby, these Privacy Act subsections would undermine SSA investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

The AF System supports our goal of enhancing SSA's fraud prevention and detection activities by protecting the public's data, providing secure online services, and increasing payment accuracy. The AF System provides us with access to a single repository of data that currently resides across many different SSA systems of records. We use the PII in the AF System to employ advanced data analytics solutions to identify patterns indicative of fraud, improve the functionality of data-driven fraud activations, conduct real-time risk analysis, and integrate developing technology into our anti-fraud business processes. This solution also provides true business intelligence to agency leadership with assistance in data-driven anti-fraud decision-making. We use the records

in the AF System to detect indications of fraud in all our programs and operations initiated by individuals outside of SSA or internal to SSA (e.g., SSA employees).

In accordance with 5 U.S.C. 552a(r), we provided a report to OMB and Congress on this modified system of records. Concurrently, in today's edition of the *Federal Register*, we are publishing a Notice of Proposed Rulemaking (NPRM), in which we propose the addition of this system of records to the list of systems exempted under the Privacy Act.¹

Matthew Ramsey,

Executive Director,

Office of Privacy and Disclosure,

Office of the General Counsel.

¹ The public may access the NPRM at www.regulations.gov and searching under the common docket folder, "SSA-2018-00012".

SYSTEM NAME AND NUMBER: Anti-Fraud (AF) System, 60-0388

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION:

Social Security Administration

Office of Analytics, Review, and Oversight

Office of Anti-Fraud Programs

Robert M. Ball Building

6401 Security Boulevard

Baltimore, MD 21235

SYSTEM MANAGER(S):

Social Security Administration

Office of Analytics, Review, and Oversight

Office of Anti-Fraud Programs

Robert M. Ball Building

6401 Security Boulevard

Baltimore, MD 21235

DCARO.OAFP.Controls@ssa.gov

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Sections 205(a) and 702(a)(5) of the Social Security Act, as amended, and the Fraud Reduction and Data Analytics Act of 2015 (Pub. L. 114-186).

PURPOSE(S) OF THE SYSTEM: The records maintained in the AF System are necessary to detect, prevent, mitigate, and track the likelihood of fraudulent activity in SSA's programs and operations. We will use information in this system to identify patterns of fraud and to improve data-driven fraud activations and real-time analysis. We may use the results of these data analysis activities, including fraud leads and vulnerabilities, in our fraud investigations and other activities to support program and operational improvements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This system maintains information about individuals who are relevant to suspicious or potentially fraudulent activities connected with Social Security programs and operations, including but not limited to, the subjects of an investigation, Social Security applicants and beneficiaries, recipients, Supplemental Security income applicants and recipients, representative payees, appointed representatives, complainants, key witnesses, and current or former employees, contractors, or agents.

CATEGORIES OF RECORDS IN THE SYSTEM: We will collect and maintain information in connection with our review of all suspicious or potentially fraudulent activities in Social Security programs and operations. We will also collect and maintain SSA and non-SSA breach information, including data generated internally or received from businesses with whom SSA has a relationship or government entities or partners.

The AF System includes records on individuals that it obtains from other SSA systems of records and will maintain information such as:

Enumeration Information: This information may include name, Social Security number (SSN), date of birth, parent name(s), address, and place of birth.

Earnings Information: This information may include yearly earnings and quarters of

coverage information.

Social Security Benefit Information: This information may include disability status, benefit payment amount, data relating to the computation, appointed representative, and representative payee.

Supplemental Security Income payment information: This information may include may include disability status, benefit payment amount, data relating to the computation, appointed representative, and representative payee.

Representative Payee Information: This information may include names, SSNs, and addresses of representative payees and relationship with the beneficiary.

Persons Conducting Business with Us Through Electronic Services: This information may include name, address, date of birth, SSN, knowledge-based authentication data, and blocked accounts.

Employee Information: This information may include a personal identification number (PIN), employee name, job title, SSN about our employees, contractors, or agents.

RECORD SOURCE CATEGORIES: We obtain information in this system from individuals (i.e., the public and SSA staff), other Government agencies, and private entities. The largest record sources for the AF System is information the agency collects and maintains for purposes related to other business processes that have established systems of records, such as the Master Files of SSN Holders and SSN Applications (60-0058), the Claims Folders System (60-0089), the Master Beneficiary Record (60-0090), the Supplemental Security Income Record and Special Veterans Benefits (60-0103), the Personal Identification Number File (60-0214), the Master Representative Payee File (60-0222), and the Central Repository of Electronic Authentication Data Master File (60-0373). The AF System may pull any relevant information from any SSA system of

records. For a full listing of our system of records notices that could provide information to the AF System, please see the Privacy Program section of SSA's website.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

We will disclose records pursuant to the following routine uses; however, we will not disclose any information defined as "return or return information" under 26 U.S.C. 6103 of the Internal Revenue Code (IRC), unless authorized by statute, the Internal Revenue Service (IRS), or IRS regulations.

1. To any agency, person, or entity in the course of an SSA investigation to the extent necessary to obtain or to verify information pertinent to an SSA fraud investigation.
2. To a congressional office in response to an inquiry from that office made on behalf of, and at the request of, the subject of the record or a third party acting on the subject's behalf.
3. To the Office of the President in response to an inquiry received from that office made on behalf of, and at the request of, the subject of record or a third party acting on the subject's behalf.
4. To the Department of Justice (DOJ), a court or other tribunal, or another party before such court or tribunal, when:
 - (a) SSA, or any component thereof; or
 - (b) any SSA employee in his or her official capacity; or

- (c) any SSA employee in his or her individual capacity where DOJ (or SSA where it is authorized to do so) has agreed to represent the employee; or
- (d) the United States or any agency thereof where SSA determines the litigation is likely to SSA or any of its components, is a party to the litigation or has an interest in such litigation, and we determine that the use of such records by DOJ, a court or other tribunal, or another party before the tribunal, is relevant and necessary to the litigation, provided, however, that in each case, we determine that such disclosure is compatible with the purpose for which the records were collected.

5. To contractors and other Federal agencies, as necessary, for the purpose of assisting us in the efficient administration of its programs. We will disclose information under this routine use only in situations in which we may enter into a contractual or similar agreement to obtain assistance in accomplishing an SSA function relating to this system of records.
6. To student volunteers, individuals working under a personal services contract, and other workers who technically do not have the status of Federal employees, when they are performing work for SSA, as authorized by law, and they need access to PII in our records in order to perform their assigned agency functions.
7. To Federal, State, and local law enforcement agencies and private security contractors, as appropriate, if necessary:
 - (a) to enable them to protect the safety of SSA employees and customers, the security of the SSA workplace, and the operation of our facilities, or

(b) to assist investigations or prosecutions with respect to activities that affect such safety and security, or activities that disrupt the operation of our facilities.

8. To the National Archives and Records Administration (NARA) under 44 U.S.C. 2904 and 2906.

9. To appropriate agencies, entities, and persons when:

(a) SSA suspects or has confirmed that there has been a breach of the system of records;

(b) SSA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, SSA (including its information systems, programs, and operations), the Federal Government, or national security; and

(c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with SSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

10. To another Federal agency or Federal entity, when we determine that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(a) responding to suspected or confirmed breach; or

(b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

11. To the Equal Employment Opportunity Commission, when requested in connection with investigations into alleged or possible discriminatory practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures, or other functions vested in the Commission.
12. To the Office of Personnel Management, Merit Systems Protection Board, or the Office of Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigations of alleged or possible prohibited personnel practices, and other such functions promulgated in 5 U.S.C. Chapter 12, or as may be required by law.
13. To the Federal Labor Relations Authority, the Office of the Special Counsel, the Federal Mediation and Conciliation Service, the Federal Service Impasses Panel, or an arbitrator requesting information in connection with the investigations of allegations of unfair practices, matters before an arbitrator or the Federal Service Impasses Panel.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: We maintain records in this system in paper and electronic form.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: We will retrieve records by the individual's name, SSN, as well as internal transaction identifiers (e.g., transaction identification for the Internet Claim application, transaction identification for an electronic online Direct Deposit change, etc.). Information from these retrieved records that matches across other agency systems of records will also create a linkage to

retrieve those records, because the system is able to show key connections or overlaps based on similar information stored in different data sources at the agency.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS: These records are currently unscheduled. We retain the records in accordance with NARA approved records schedules. In accordance with NARA rules codified at 36 CFR 1225.16, we maintain unscheduled records until NARA approves an agency-specific records schedule or publishes a corresponding General Records Schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: We retain electronic and paper files containing personal identifiers in secure storage areas accessible only by our authorized employees who have a need for the information when performing their official duties. Security measures include, but are not limited to, the use of codes and profiles, personal identification number and password, and personal identification verification cards. We restrict access to specific correspondence within the system based on assigned roles and authorized users. We maintain electronic files with personal identifiers in secure storage areas. We will use audit mechanisms to record sensitive transactions as an additional measure to protect information from unauthorized disclosure or modification. We keep paper records in cabinets within secure areas, with access limited to only those employees who have an official need for access in order to perform their duties.

We annually provide our employees and contractors with appropriate security awareness training that includes reminders about the need to protect PII and the criminal penalties that apply to unauthorized access to, or disclosure of PII. See 5 U.S.C. 552a(i)(1). Furthermore, employees and contractors with access to databases maintaining

PII must annually sign a sanction document that acknowledges their accountability for inappropriately accessing or disclosing such information.

RECORD ACCESS PROCEDURES: This system of records is exempt from the Privacy Act's access, contesting, and notification provisions stated below. However, individuals may submit requests for information about whether this system contains a record about them by submitting a written request to the system manager at the above address, which includes their name, SSN, or other information that may be in this system of records that will identify them. Individuals requesting notification of, or access to, a record by mail must include (1) a notarized statement to us to verify their identity or (2) must certify in the request that they are the individual they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another individual under false pretenses is a criminal offense.

Individuals requesting notification of or access to, records in person must provide their name, SSN, or other information that may be in this system of records that will identify them, as well as provide an identity document, preferably with a photograph, such as a driver's license. Individuals lacking identification documents sufficient to establish their identity must certify in writing that they are the individual they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another individual under false pretenses is a criminal offense.

These procedures are in accordance with our regulations at 20 CFR 401.40 and 401.45.

CONTESTING RECORD PROCEDURES: Same as record access procedures. Individuals should also reasonably identify the record, specify the information they are contesting, and state the corrective action sought and the reasons for the correction with

supporting justification showing how the record is incomplete, untimely, inaccurate, or irrelevant. These procedures are in accordance with our regulations at 20 CFR 401.65(a).

NOTIFICATION PROCEDURES: Same as record access procedures. These procedures are in accordance with our regulations at 20 CFR 401.40 and 401.45.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: This system of records is exempt from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in today's Federal Register.

HISTORY: Anti-Fraud Enterprise Solution (AFES), 83 FR 19588.

[FR Doc. 2020-26753 Filed: 12/10/2020 8:45 am; Publication Date: 12/11/2020]