SYSTEM NAME AND NUMBER: Unclaimed Deposit Account Records, FDIC-024.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at FDIC facilities in Arlington, Virginia and regional offices. Original and duplicate systems may exist, in whole or in part, at secure sites and on secure servers maintained by third-party service providers for the FDIC.

SYSTEM MANAGER(S): Financial Managers, Division of Resolutions and Receiverships, FDIC, 550 17th Street NW, Washington, DC 20429, and 600 North Pearl Street, Suite 700, Dallas, Texas 75201.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Sections 9, 11, and 12 of the Federal Deposit Insurance Act (12 U.S.C. 1819, 1821, and 1822).

PURPOSE(S) OF THE SYSTEM: The information in this system is used to process inquiries and claims of individuals with respect to unclaimed insured deposit accounts of closed insured depository institutions for which the FDIC was appointed receiver after January 1, 1989, and to assist in complying with the requirements of the Unclaimed Deposits Amendments Act.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals identified as deposit account owners and individuals claiming to be deposit account holders of unclaimed insured deposits of a closed insured depository institution for which the FDIC was appointed receiver after January 1, 1989.

CATEGORIES OF RECORDS IN THE SYSTEM: Deposit account records, including signature cards; last known home address; social security number; name of insured depository institution.

RECORD SOURCE CATEGORIES: Information originates from deposit records of closed insured depository institutions and claimants. After 18 months following institution failure, unclaimed deposit records are transferred to the FDIC from assuming depository institutions. Custody of these records are transferred to State's unclaimed property for a period of 10 years. After 10 years, unclaimed records are returned to FDIC.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the FDIC as a routine use as follows:

(1) To appropriate Federal, State, local and foreign authorities responsible for investigating or prosecuting a violation of, or for enforcing or implementing a statute, rule, regulation, or order issued, when the information indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto;

(2) To a court, magistrate, or other administrative body in the course of presenting evidence, including disclosures to counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal proceedings, when the FDIC is a party to the proceeding or has a significant interest in the proceeding, to the extent that the information is determined to be relevant and necessary;

(3) To a congressional office in response to an inquiry made by the congressional office at the request of the individual who is the subject of the record;

(4) To appropriate agencies, entities, and persons when (a) the FDIC suspects or has confirmed that there has been a breach of the system of records; (b) the FDIC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the FDIC (including its information systems, programs, and operations), the Federal Government, or national security; the FDIC and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the FDIC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm;

(5) To another Federal agency or Federal entity, when the FDIC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a 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.

(6) To appropriate Federal, State, and local authorities in connection with hiring or retaining an individual, conducting a background security or suitability investigation, adjudication of liability, or eligibility for a license, contract, grant, or other benefit;

(7) To appropriate Federal, State, and local authorities, agencies, arbitrators, and other parties responsible for processing any personnel actions or conducting

administrative hearings or corrective actions or grievances or appeals, or if needed in the performance of other authorized duties;

(8) To appropriate Federal agencies and other public authorities for use in records management inspections;

(9) To officials of a labor organization when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;

(10) To contractors, grantees, volunteers, and others performing or working on a contract, service, grant, cooperative agreement, or project for the FDIC, the Office of Inspector General, or the Federal Government for use in carrying out their obligations under such contract, grant, agreement or project;

(11) To the appropriate State agency accepting custody of unclaimed insured deposits; and

(12) To allow members of the public access to a limited portion of the data sufficient to help individuals locate and understand the status of their accounts previously held by a financial institution.

(13) To Federal agencies, and to those Federal employees designated by the President or Agency Heads pursuant to Executive Order 14243, for the purposes of identifying and eliminating waste, fraud, and abuse, including the elimination of bureaucratic duplication and inefficiency and the enhancement of the Government's ability to detect overpayments and fraud.

(14) To the U.S. Department of the Treasury when disclosure of the information is relevant to review payment and award eligibility through the Do Not Pay

Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state (meaning a state of the United States, the District of Columbia, a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored in electronic media and in paper format within individual file folders.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Electronic media and paper format are indexed and retrieved by depository institution name, depositor name, depositor social security number, or deposit account number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records of unclaimed deposits are maintained ten years after the termination date of the receivership or as established by the state or Federal law or court order, if longer. Disposal is by shredding or other appropriate disposal methods.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records are protected from unauthorized access and improper use through administrative, technical, and physical security measures. Administrative safeguards include written guidelines on handling personal information including agency-wide procedures for safeguarding personally identifiable information. In addition, all FDIC staff are required to take annual privacy and security training. Technical security measures within FDIC include restrictions on computer access to authorized individuals who have a legitimate need to know the information; required use of strong passwords that are frequently changed; multi-factor authentication for remote access and access to many FDIC network

components; use of encryption for certain data types and transfers; firewalls and intrusion detection applications; and regular review of security procedures and best practices to enhance security. Physical safeguards include restrictions on building access to authorized individuals, security guard service, and maintenance of records in lockable offices and filing cabinets.

RECORD ACCESS PROCEDURES: Individuals wishing to request access to records about them in this system of records must submit their request in writing to the FDIC FOIA & Privacy Act Group, 550 17th Street, NW, Washington, DC 20429, or email *efoia@fdic.gov*. Requests must include full name, address, and verification of identity in accordance with FDIC regulations at 12 CFR part 310.

CONTESTING RECORD PROCEDURES: Individuals wishing to contest or request an amendment to their records in this system of records must submit their request in writing to the FDIC FOIA & Privacy Act Group, 550 17th Street, NW, Washington, DC 20429, or email *efoia@fdic.gov*. Requests must specify the information being contested, the reasons for contesting it, and the proposed amendment to such information in accordance with FDIC regulations at 12 CFR part 310.

NOTIFICATION PROCEDURES: Individuals wishing to know whether this system contains information about them must submit their request in writing to the FDIC FOIA & Privacy Act Group, 550 17th Street, NW, Washington, DC 20429, or email *efoia@fdic.gov*. Requests must include full name, address, and verification of identity in accordance with FDIC regulations at 12 CFR part 310.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 80 FR 66981 (Oct. 30, 2015), 84 FR 35184 (Jul. 22, 2019); 87 FR 66181 (Nov. 2, 2022).