SYSTEM NAME AND NUMBER:

Office of Inspector General Files–FTC (FTC-I-7).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of Inspector General (OIG), Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems and at 87 FR 57698 (Sept. 21, 2022). Also see https://www.ftc.gov/office-inspector-general/reports-correspondence.

SYSTEM MANAGER(S):

Inspector General, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, email: SORNs@ftc.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Inspector General Act, as amended, 5 U.S.C. 401 et seq.

PURPOSE(S) OF THE SYSTEM:

The OIG maintains this system of records to carry out its responsibilities pursuant to the Inspector General Act, as amended. The OIG is statutorily directed to receive complaints and conduct and supervise investigations, reviews and audits relating to programs and operations of the Federal Trade Commission, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, the records in this system consist of complaints and related correspondence concerning possible violations of law, rules, regulations, mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health or

safety related to the FTC; records created, received, or obtained during the course of investigating individuals and entities suspected of having committed illegal or unethical acts or misconduct and in any resulting related criminal prosecutions, civil proceedings, or administrative actions; and records created, received, or obtained during the course of conducting audits, inspections, or reviews and issuing reports, advisories or correspondence.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered consist of: (1) current and former FTC employees, applicants for employment, contractors and subcontractors associated with an activity that OIG is investigating, inspecting, reviewing, or auditing; (2) individuals who submit complaints to the OIG; (3) subjects of hotline complaints; and (4) individuals and entities performing some other role of significance to the OIG's investigative, inspecting, reviewing, or auditing efforts, such as potential witnesses or subjects who are not FTC current or former employees, contractors or subcontractors. The system also tracks information related to OIG staff and staff of other agencies involved in conducting the investigative, inspecting, reviewing or auditing activity.

CATEGORIES OF RECORDS IN THE SYSTEM

Records related to complaints to the OIG, planning and conducting investigations, reviews, inspections and audits, the results of investigations, and any civil, criminal, or administrative actions resulting from investigations and other matters. More specifically, this includes, but is not limited to, correspondence relating to investigations and other matters; internal staff memoranda; copies of subpoenas issued during investigations and other matters, affidavits, statements from witnesses, transcripts of testimony taken in investigations or other matters and accompanying exhibits; documents, records or copies obtained during investigations and other matters; interview notes, documents and records relating to investigations and other matters; opening reports, information or data relating to alleged or suspected criminal, civil or administrative violations or similar wrongdoing by subject individuals and final reports of investigation and other matters.

RECORD SOURCE CATEGORIES:

Employees or other individuals on whom the record is maintained, non-target witnesses, FTC and non-FTC records, to the extent necessary to receive, review and respond to complaints and carry out OIG investigations, reviews, inspections, and audits, as authorized by 5 U.S.C. 401 et seq.

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

Records in this system may be:

1. Disclosed to agencies, offices, or establishments of the executive, legislative, or judicial branches of the federal or state government–

   (a) Where such agency, office, or establishment has an interest in the individual for employment purposes, including a security clearance or determination as to access to classified information, and needs to evaluate the individual's qualifications, suitability, and loyalty to the United States Government, or

   (b) Where such agency, office, or establishment conducts an investigation of the individual for the purposes of granting a security clearance, or for making a determination of qualifications, suitability, or loyalty to the United States Government, or access to classified information or restricted areas, or

   (c) Where the records or information in those records are relevant and necessary to a decision with regard to the hiring or retention of an employee or disciplinary or other administrative action concerning an employee, or

   (d) Where disclosure is requested in connection with the award of a contract or other determination relating to a government procurement, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the record is relevant and necessary to the requesting agency's decision on the matter, including, but not limited to,

disclosure to any Federal agency responsible for considering suspension or debarment actions where such record would be germane to a determination of the propriety or necessity of such action, or disclosure to the United States General Accountability Office, the General Services Administration Board of Contract Appeals, or any other federal contract board of appeals in cases relating to an agency procurement.

2. Disclosed to the Office of Personnel Management, the Office of Government Ethics, the Merit Systems Protection Board, the Office of the Special Counsel, the Equal Employment Opportunity Commission, or the Federal Labor Relations Authority or its General Counsel, of records or portions thereof relevant and necessary to carrying out their authorized functions, such as, but not limited to, rendering advice requested by the OIG, investigations of alleged or prohibited personnel practices (including unfair labor or discriminatory practices), appeals before official agencies, offices, panels or boards, and authorized studies or review of civil service or merit systems or affirmative action programs.
3. Disclosed to independent auditors or other private firms with which the Office of the Inspector General has contracted to carry out an independent audit or investigation, or to analyze, collate, aggregate or otherwise refine data collected in the system of records, subject to the requirement that such contractors shall maintain Privacy Act safeguards with respect to such records.
4. Disclosed to a direct recipient of federal funds such as a contractor, where such record reflects serious inadequacies with a recipient's personnel and disclosure of the record is for purposes of permitting a recipient to take corrective action beneficial to the Government;
5. Disclosed to any official charged with the responsibility to conduct qualitative assessment reviews of internal safeguards and management procedures employed in investigative operations. This disclosure category includes members of the Council of the Inspectors General on Integrity and Efficiency and officials and administrative staff within their investigative chain of command, as well as authorized officials of the Department of Justice

and the Federal Bureau of Investigation;

6. Disclosed to members of the Council of the Inspectors General on Integrity and Efficiency for the preparation of reports to the President and Congress on the activities of the Inspectors General;
7. Disclosed to complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or which they were a victim.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems and at 83 FR 55541, 55542-55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The FTC maintains system records in various electronic and non-electronic formats and media. The OIG Files consist of paper records maintained in file folders, cassette tapes and CD-ROMs containing audio recordings of investigative interviews, and data maintained on computer diskettes and hard drives. The folders, cassette tapes, CD-ROMs and diskettes are stored in file cabinets in the OIG. Electronic files are retained either in FTC servers or on the cloud.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The records are retrieved by the name of the subject of the investigation or by a unique control number assigned to each investigation.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with Schedule DAA-0122-2020-0001, which was approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access is restricted to agency personnel or contractors whose responsibilities require access. Access to electronic records is controlled by "user ID" and password combination, and/or role-based access controls, and/or other electronic access or network controls (e.g., firewalls). Paper records are maintained in lockable rooms or file cabinets, which are kept locked during non-duty hours. FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems and at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems and at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(j)(2), records in this system are exempt from the provisions of 5 U.S.C. 552(a), except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10) and

(11) and (i) and corresponding provisions of 16 CFR 4.13, to the extent that a record in the system of records was compiled for criminal law enforcement purposes.

Pursuant to 5 U.S.C. 552a(k)(2), the system is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I) and (f) and the corresponding provisions of 16 CFR 4.13, to the extent the system of records consists of investigatory material compiled for law enforcement purposes, other than material within the scope of the exemption at 5 U.S.C. 552a(j)(2). See 16 CFR 4.13(m).

HISTORY:

89 FR 79598-79610 (September 30, 2024)

74 FR 17863-17866 (April 17, 2009)

73 FR 33591-33634 (June 12, 2008).