

SYSTEM NAME AND NUMBER:

Call Detail Records–FTC (FTC-VII-4).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

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/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 80 FR 9460, 9465 (Feb. 23, 2015).

SYSTEM MANAGER(S):

Core Engineering and ISSO Services Program Manager, Office of the Chief Information Officer, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, email: SORNs@ftc.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 et seq.

PURPOSE(S) OF THE SYSTEM:

To manage agency telecommunications resources; to monitor appropriate use of such resources; to detect and deter possible improper or unauthorized use of such resources; in cases where such use is detected, to determine whether disciplinary or other action, assessment, charge, or referral is warranted; to determine appropriate types and levels of service that should be available to agency staff; and to review and authorize payment of telecommunications invoices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

FTC personnel, consultants, and contractors assigned office telephones, cell phones, telephone calling cards, pagers or other telecommunications resources.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name, office telephone number, cell phone number, telephone calling card number, pager number, originating telephone number, telephone numbers called, length of telephone calls, cost of telephone calls.

RECORD SOURCE CATEGORIES:

Telephone assignment records; computer software that captures telephone call information and permits query and reports generation; logs, reports, or other service records that the FTC may receive from telecommunications service providers.

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

Records in this system may be disclosed:

(1) To a telecommunications company and/or the General Services Administration when providing the FTC with telecommunications support in order to verify billing or perform other servicing to the account; and

(2) To respond to a Federal agency's request made in connection with the hiring or retention of an employee, the letting of a contract or issuance of a grant, license or other benefit by the requesting agency, but only to the extent that the information disclosed is relevant and necessary to the requesting agency's decision on the matter.

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/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 83 FR 55542-55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Maintained in paper and/or other digital or non-digital formats.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed by office telephone number, cell phone number, pager number, or telephone calling card number, or individual's name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

See National Archives and Records Administration General Records Schedule 3.1, item 020, regarding information technology operations and maintenance records which are destroyed three years after project completion, but longer retention is authorized if required for business use. See GRS 5.5, item 20, regarding mail, printing, and telecommunication services control records that are retained for one year, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access is restricted to agency and contractor personnel whose official responsibilities require access. Paper records are maintained in lockable cabinets or offices. Access to electronic records is protected by "user ID" and password combination and/or other electronic access and network controls (e.g., firewalls). 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/about-ftc/foia/foia-reading-rooms/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/about-ftc/foia/foia-reading-rooms/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/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

80 FR 9460-9465 (February 23, 2015)

74 FR 17863-17866 (April 17, 2009)

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