Federal Trade Commission
Privacy Impact Assessment
Redress Enforcement Database (RED)

August 2015

1 System Overview

The Federal Trade Commission's (FTC or Commission) Bureau of Consumer Protection (BCP) enforces many of the nation's consumer protection laws and works to protect consumers from a variety of fraudulent, deceptive, and unfair practices in the marketplace. To further its consumer protection mission, BCP brings law enforcement actions in federal court and in administrative proceedings, and provides consumer and business education to enable the public to avoid common harms.

BCP's Division of Enforcement (DE) and Redress Administration Office (RAO) jointly working with the Office of the Chief Information Officer (OCIO) and with OCIO's contractors, created the Redress and Enforcement Database System (RED). The RED collects and maintains information, including personally identifiable information (PII), relating to defendants against whom the FTC has obtained judgments and/or injunctive orders in legal proceedings brought under the FTC Act and other statutes and rules enforced by the FTC. The information enables the Commission to monitor compliance with injunctive orders, collect outstanding judgments, and, when possible, return recovered funds to victimized consumers and businesses.

Division of Enforcement
DE uses the RED to support its mission of enforcing judgments and orders obtained in FTC consumer protection actions. The RED collects, secures, and permits authorized FTC staff to review records concerning defendants who are subject to judgments and/or orders obtained in FTC actions, details of final judgments or orders entered as to those defendants, actions undertaken by DE (and other FTC staff, where applicable) in monitoring defendants' compliance with those orders and collecting upon judgments and other orders providing for monetary relief, and the status of those activities. The RED contains related information that improves DE's ability to enforce judgments and orders, including contact information for defendants; their attorneys, agents, employers, successors, and associates; and entities who have facilitated defendants' financial transactions. These entities may possess information about defendants' activities or be required by law to comply with orders issued in FTC actions. (For example, successors may be required to comply with an order as successors-in-interest, and associates and other entities may be required to comply with orders pursuant to Federal Rule of Civil Procedure 65.) DE also uses the RED to maintain contact information for other law enforcement authorities who have expressed an interest in FTC actions and to locate contact information for federal, state, and local law enforcement authorities who may also be interested in investigating entities within their jurisdictions that are under FTC order. Additionally, DE uses the RED to collect and maintain information pertaining to bankruptcy actions initiated by or pertaining to FTC defendants.

Redress Administration
RAO uses the RED to collect and track information related to redress, and to conduct oversight of the contractors who assist the FTC in administering redress to consumers and businesses. RAO collects the estimated dollar loss and number of affected consumers in the RED and uses the information to estimate the cost for distributing redress payments and/or mailing consumer education material. If redress is practicable, RAO uses the RED to prepare cost estimates, generate work assignments, and approve administrative invoices. The redress contractors enter data from bank statements that contain money obtained by the FTC for refunds to consumers.

The RED also imports the following financial data from the FTC's Financial Management Office (FMO) accounting system – money collected, distributed, and expensed, and unused redress funds. Finally, the RED also contains contact information and related data regarding receivers appointed in FTC actions, which may be used to help identify potential receivers for future FTC actions.

RED System

The RED uses the Oracle Relational Database Management System to create a secure data repository. The RED is accessible on the FTC network via a secure internal web-based interface and is hosted in the FTC's Data Center General Support System.[1] The RED minimizes the manual keying and re-keying of relevant data in several ways. First, it sends an automated email to a case manager containing a link to an internal, web-based questionnaire (E-Survey), enabling the case manager to input relevant data. The questionnaire can only be accessed and completed after the case manager enters their RED login credentials, and the link cannot be forwarded or used by unapproved recipients. Second, RED transfers relevant data from existing FTC systems using database links, including the Matter Management System (MMS)[2] and the agency's Financial Management Office (FMO) accounting system. Data travels in only one direction, from MMS/FMO to RED, and RED employs private database links and is limited to read-only access to MMS and FMO. Additionally, RED limits the access rights to the administrative interface solely to RAO, DE staff and other FTC users specifically authorized to access the interface. Authorized users have the ability to read or modify data only if they have been specifically granted such rights within the RED for business purposes, and all modifications, revisions, and deletions of data are logged.

While there is some data in the RED that relates to both missions, the interface segregates data relating solely to RAO's mission from data relating solely to DE's mission. Access to either organization's data is provided by that organization only to authorized users on a least-privilege-access, need-to-know basis. The RED access and authorization permissions are maintained within the RED by the RAO and DE administrators.

2 Information Collected and Stored within the System

2.1 What information is to be collected, used, disseminated, or maintained by the system?

Division of Enforcement

The RED compiles and maintains records relating to defendants who are subject to judgments and/or orders obtained in FTC consumer protection actions; the contents of those judgments or orders; actions taken by DE (and other FTC staff, where applicable) in monitoring defendants' compliance with those orders and collecting upon judgments and other orders providing for monetary relief; the status of such activities; law enforcement authorities who have expressed an interest in particular FTC actions; and bankruptcy actions initiated by or pertaining to FTC

[1] For more information, refer to the Data Center General Support System PIA at https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

[2] For more information, refer to the MMS PIA at https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

defendants. No documents are included in the RED itself; the RED contains links to relevant documents on FTC shared drives, for which the user must have separate access privileges.

The personal information collected about defendants contained in the RED may include names, addresses, social security numbers (SSNs); dates of birth; employer identification numbers (EINs); home and work phone numbers, email addresses, facsimile numbers; and contact information for defendants' employers. For some matters, RED may include photographs to permit identification of defendants. In addition, the RED includes contact information for defendants' attorneys, agents, successors, associates, and entities who have facilitated defendants' financial transactions; these entities often possess information about defendants' commercial activities and, in certain circumstances, may be required by law to comply with an injunctive order obtained against an FTC defendant.

The information collected for each judgment or order includes the following: (a) the date that each judgment or order was entered; (b) the judge and court that entered the order; (c) the parties bound by the order; (d) the statute, products, and alleged violations at issue in the action; (e) the contact information and fields of expertise of any expert witnesses retained in the action; (f) the legal basis for any monetary relief in the order; (g) an identification of any bans, bonds, monetary provisions, or suspended judgments imposed under the order; (h) and a statement of whether there are any protective orders or centrally-archived paper records pertaining to the case.

The compliance information collected for each order and defendant includes the following: (a) the date that the order was served on each defendant; (b) the date that each defendant delivers to the FTC the acknowledgments of service and compliance reports required by the order; (c) the due dates for compliance reports; a statement of the frequency of FTC review of order compliance; (d) the duration of record keeping and compliance monitoring requirements set forth in the order; (e) the status of compliance monitoring activities; (f) and an identification of other persons served with the order. To assist staff in reviewing defendants' compliance with injunctive orders, RED tracks whether defendants have submitted compliance reports in a timely manner and also identifies defendants whose compliance monitoring provisions may be expiring.

The collections-related information for each defendant subject to a judgment or other order providing for monetary relief includes the following: (a) the date the relief was awarded; (b) the total amount of the award; (c) the amount of the award, if any, that is suspended; (d) the unsuspended amount that the defendant is obligated to pay; (e) the amount(s) collected by the FTC and the method(s) used to collect those sums; (f) the estimated amount owed by the defendant; (g) and the dates of events in the collections process.

Information about other law enforcement authorities who have expressed an interest in FTC actions includes those authorities' contact information and summary information regarding criminal actions brought against FTC defendants, including case numbers, indictment dates, conviction dates, and criminal sentences imposed against FTC defendants. The system also identifies defendants who have received a warning letter from the U.S. Food and Drug Administration (FDA).

Bankruptcy information includes summary information concerning bankruptcy proceedings initiated by or pertaining to FTC defendants, such as bankruptcy petition dates and chapters,

courts, case numbers, deadlines and dates for non-dischargability complaints and proofs of claims, whether debtors were discharged, and whether bankruptcy cases were closed or dismissed.

Redress Administration
The RED tracks broad categories of information concerning redress. For example, the system compiles and maintains information concerning the amount of the judgment debt, the date that the judgment becomes due, payments received, and debt delinquency or default. It also contains information regarding the number and total dollar amount of redress distributions, the number of consumers receiving redress, the percentage of loss refunded to consumers, and the fees and costs associated with distributing redress. The RED also contains contact information and related data concerning receivers appointed in particular cases.

In addition to the redress and enforcement information referenced above, the system logs each individual who enters, revises or deletes information; the system also logs the time and date of user sessions (although it does not log specific queries or views).

2.2 What are the sources of the information in the system?

Division of Enforcement
Judgment and order information is obtained from court orders. The defendant's personal information is obtained by FTC staff during the course of investigation and/or order compliance monitoring. Personal information may be collected directly from the individuals and businesses that are the targets of FTC law enforcement actions or from financial statements that defendants may be required to produce. Financial transactions recorded by FMO are obtained by FMO. In addition, the FTC may receive personal information in the course of litigation or during settlement negotiations. The FTC also may obtain information from credit reporting agencies, publicly available databases (such as Lexis/Nexis), or federal, state, or local agencies furnishing identifying information. Information on FDA warning letter recipients is provided by the FDA.

Redress Administration
Information about the amount of consumer loss in a specific matter is provided by the FTC case manager. The fees and costs associated with distributing redress are defined in the contracts the FTC has with contractors who assist the agency in administering redress to consumers.

2.3 Why is the information being collected, used, disseminated, or maintained?

Division of Enforcement
DE collects the above information (see Section 2.1) to maintain records about individuals who are named in orders obtained by the agency, who may be subject to such orders, or who owe money to the FTC, so that the FTC may monitor compliance with and enforce existing judgments and injunctive orders, and report on its activities. Information such as SSNs, dates of birth, and identification photographs are necessary to accurately monitor defendants, confirm that individual defendants are correctly identified, and to ensure that any communication with the Department of Treasury identifies the correct individual. DE may obtain contact and identification information such as SSNs, dates of birth, addresses, and phone numbers from publicly available commercial data to assist DE staff in locating, contacting, and monitoring defendants bound by FTC orders.

The FTC also collects address information for defendants' successors and associates, as well as financial entities that facilitate defendants' transactions, in order to maintain a record of persons or entities who may have information about the defendants' commercial activities or who may be required by law (pursuant to Federal Rule of Civil Procedure 65 or otherwise) to comply with an order obtained by the FTC.

DE collects contact information of other law enforcement authorities to facilitate communication with those authorities and identify law enforcement authorities who may also investigate entities bound by orders in FTC actions. Information on FDA warning letter recipients is no longer cross-checked against FTC defendants to identify whether any FTC defendants have received FDA advisories that may relate to their compliance with an order obtained by the FTC.

DE collects summary information about bankruptcy proceedings relating to FTC defendants to assist its staff of bankruptcy specialists who advise other FTC staff with respect to such proceedings.

Redress Administration
RAO uses RED to track case management information. This information includes billing units and fees related to FTC's contracts with contractors who assist in administering redress. This data is used in cost estimating, issuing work assignments, and approving redress contractor invoices. The RED tracks milestones and case notes to measure RAO performance compared to the Government Performance and Results Act.

RAO uses the RED to collect data for other offices within the FTC. RAO enters receivership contact information for use by FMO, and FMO mails surveys to receivers to track financial activity. FMO collects estimates on collectability of defendants' debts from case managers so it can record allowances for uncollectible accounts. RAO also tracks total dollars and checks issued by country within each matter. RAO provides data involving checks issued to consumers in foreign countries ("Foreign Claimant data") to the FTC's Office of International Affairs (OIA); this includes the matter number, the foreign country, and the sum total in dollar amount paid out in that country (but not information about the individuals to whom redress was paid). Active bank account information is provided to the FTC's Office of Inspector General (OIG) for confirmation letters as part of the annual audit of redress funds.

2.4 How is the information collected?

Division of Enforcement
Information is collected by BCP case managers who review the legal documents and information associated with a case and enter relevant information into the RED. The case managers enter data via an electronic, web-based questionnaire tool (E-Survey) made available via the FTC's intranet. They may also submit relevant documents via internal FTC email; as noted earlier, no documents are included in the RED, which instead contains restricted links to those documents on the FTC shared drives requiring separate access privileges. DE and other authorized FTC staff also input information into the RED in the course of monitoring defendants' compliance with final orders; this information is summarized in section 2.1 above. In addition, data is entered by transferring relevant data from the FTC's Matter Management System and FMO's financial system to the RED.

Redress Administration
RAO enters cashed redress checks and banking and checking data (including matter name and bank name) reported from bank statements. Financial data from FMO is imported from the agency's financial system into the database. In addition, case management data is entered by RAO based on discussions with case managers. Foreign Claimant data provided by FTC-approved redress contractors is also entered into the database by RAO. Finally, receiver data is entered using information from court orders and E-Surveys completed by FTC case managers.

2.5 How will the information be checked for accuracy and timeliness (currency)?

When BCP case managers reply to an E-Survey, the information is reviewed by administrators, supervisors, and/or program staff in DE and/or RAO. When all the necessary data elements are provided, RAO and DE enter the data into the RED. If information is missing from an E-Survey, DE or RAO staff contacts the case manager to correct the deficiency. DE staff assigned to monitor defendants' compliance with an order or judgment review the data in that matter for accuracy and currency. RAO enters case management data daily as the status of the case changes. The case status reports are discussed with redress contractors monthly to verify check accuracy and plan redress activity.

Data from MMS and FMO are imported daily. RAO reconciles financial data from FMO and bank statements regularly.

U.S. Department of Treasury referral data is verified at time of entry and updated on a quarterly basis.

Receiver data and Foreign Claimant data are checked by RAO annually. Photographs identifying individual defendants, when included in a matter, are retained in RED for 10 years and then automatically purged from the system.

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards,

etc.)? If so, how does the use of this technology affect individuals' privacy?

No. The system uses technologies in ways that the Commission has previously employed.

2.7 What law or regulation permits the collection of this information?

The Federal Trade Commission Act, 15 U.S.C. §§ 41-58, authorizes the FTC to collect and store this information.

In addition, pursuant to a Memorandum of Understanding (MOU) prepared in connection with the Debt Collection Improvements Act of 1996 (DCIA), 31 U.S.C. § 3720B - 3720E, the FTC must send eligible judgments that are no longer being litigated and that have been outstanding and delinquent for 180 days or more to the U.S. Department of Treasury for collection. The Treasury requires the FTC to provide each judgment debtor's name and SSN or EIN. The FTC must collect SSNs and EINs in connection with tax reporting requirements for judgment defendants (31 U.S.C. § 7701). If a debt referred to Treasury is not collectible, Treasury may issue 1099-C forms to each defendant who has not paid an outstanding judgment in full.

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

The system is used only for internal purposes (subject to the information in Section 3.3 below), and the FTC maintains safeguards to protect this information as described below. Risks to privacy arise primarily from internal threats to the information contained within the RED database, which include the unauthorized or inadvertent release of PII and unauthorized browsing for information. Several safeguards have been implemented to mitigate these risks, and to prevent the unauthorized disclosure of PII from the RED.

First, only FTC staff and contractors with an OCIO-issued user-identification and strong password can access the FTC network where the RED is housed. Furthermore, users of the FTC network need additional authorization to access the RED. Section 6.5 below provides additional information about how users obtain authorization to use the RED. The RED administrators in DE and RAO limit the ability to view, add, change, or delete information by limiting access to the RED and by establishing user roles within the RED. The RED also restricts the ability to view the E-Survey for a particular case to a single individual, usually the case manager assigned to that case. These restrictions help to protect the information in the RED from unauthorized access and from internal threats.

Second, the server on which the database is stored is protected by a firewall and other logical controls, and the RED can only be accessed through the FTC network; there is no way to directly access the RED from outside the Commission.

Third, the RED interface segregates data relating solely to RAO's mission from data relating solely to DE's mission. Access to either organization's data is provided by that organization to authorized users on a least-privilege access, need-to-know basis.

The FTC strives to collect and include within the RED only the information that is necessary to carry out the enforcement, collection, and redress functions. FTC staff, in consultation with the Chief Privacy Officer, have reviewed the RED data elements and determined that each is necessary and must be collected.

3 Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

The FTC uses information in the RED to monitor compliance with and enforce FTC judgments and orders, and to collect assets from defendants who have defrauded or otherwise victimized consumers and who are subject to a judgment or other order providing for monetary relief in an FTC law enforcement action. The FTC may also use the information about defendants, and their agents, successors, associates, and financial facilitators, for internal reporting purposes, to pursue corollary investigations, to meet tax reporting obligations, and for other uses as described by the FTC's System of Records Notices (SORNs). *See infra* Section 8. The FTC uses the contact information of receivers to identify parties who can assist the FTC and the court in cases where defendants' assets are to be frozen, marshaled, or liquidated. The FTC uses the contact information of law enforcement personnel to identify and contact those authorities with respect to FTC actions.

3.2 Which internal entities will have access to the information?

The RED may be accessed by case managers, RAO and DE staff, other authorized FTC staff in BCP or the FTC's Regional Offices, and OCIO database contractors. Separate categories of FTC users have different levels of defined access privileges on a least-privilege access, need-to-know basis. There are roles for RAO/DE administrators, RAO/DE staff (read/write access), authorized FTC Regional Office staff (read/write or read-only access as determined by FTC management); and case managers (access to complete E-Surveys only). Users authorized to access the RAO data maintained in the system use a separate web interface than the web interface used by users with authorized access to DE data, in order to limit access to each organization's data. System administrators in OCIO can upload information from MMS and the FMO accounting system into the RED, as well as correct data at the direction of RAO/DE administrators. FMO staff has read-only access to the RED. In addition, data from the RED may be requested by the OIG for internal audits. Lastly, OCIO contractors may be authorized to access data in the RED to perform technical work relating to the development and maintenance of the system. The OCIO contractors are bound by non-disclosure agreements prohibiting unauthorized disclosure of information collected by the agency.

3.3 Which external entities will have access to the information?

No external entities have direct access to the database. RAO or DE may provide data or reports from the RED to external entities as described below.

Redress Contractors
The RED contract data is used to prepare work assignments that RAO sends to redress contractors. The RED contract data is also used to review administrative and tax invoices from redress contractors.

The U.S. Department of Treasury
FTC discloses defendant data collected in the RED to the U.S. Department of Treasury when it refers eligible defendants to that agency for further collection of judgments. The U.S. Department of Treasury may share this information with the U.S. Department of Justice or with any of the private collection agencies that it may assign to collect the FTC debt. Monies collected by the U.S. Department of Treasury, DOJ, or private collection agencies will ultimately be used (if feasible and appropriate) for consumer redress. If a debt proves to be uncollectible, the U.S. Department of Treasury may then issue 1099-C forms to each defendant who has not paid a judgment in full. The RED does not collect or maintain copies of issued 1099-C forms that the Department of Treasury issues. However, case managers have the option to note in the RED that a 1099-C form has been issued.

External Law Enforcement
The FTC may disclose relevant information in the RED to other federal, state, local, or international law enforcement agencies in the course of a law enforcement investigation or action, in accordance with FTC policies and procedures for sharing non-public information.

Agents of the FTC or Courts
The FTC may disclose information in the RED to third parties employed by the FTC as agents for purposes of serving legal process or other documents or information upon defendants or third parties in litigation. Additionally, the FTC may be required or authorized to share information collected in the RED with court-appointed receivers, who are agents of the courts.

Other Disclosures
The FTC may be required or authorized to share certain data collected in the RED in other circumstances, including in response to requests from Congress, Freedom of Information Act (FOIA) requests, requests from the media (not obtained through a FOIA request), or during litigation. In these situations, the FTC redacts personal identifying information pursuant to agency policy and any applicable rules or orders of court before providing data.

4 Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

To the extent that the FTC attempts to collect information directly from defendants and related persons or entities through investigation, litigation, or voluntary settlement negotiations, these persons or entities have notice of the FTC's efforts and an opportunity to decline cooperation

or to assert a privilege or immunity from providing this information. In the context of voluntary settlement negotiations, the FTC may require defendants to provide such information under penalty of perjury in a personal financial statement. FTC final judgments resulting from negotiated settlements often contain standard language, similar to the following, informing defendants that the information may be used for collection:

> *In accordance with 31 U.S.C. § 7701, Defendants are hereby required, unless they have done so already, to furnish to the Commission their respective taxpayer identifying numbers (social security numbers or employer identification numbers), which shall be used for purposes of collecting and reporting on any delinquent amount arising out of Defendants' relationship with the government.*

Defendants indicate their consent to the collection and use of their information by signing the final judgment.

To the extent the FTC obtains personal information concerning defendants and related persons or entities from third parties and other sources, such as other law enforcement agencies or private credit reporting agencies, or public sources, defendants and related persons or entities may not have notice or an opportunity to consent to the collection or use of the information.

4.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals that provide the FTC with information on a voluntary basis may choose to decline to provide such information. However, individuals do not have a right to decline to provide information that is required by law and/or court order.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Individuals generally do not have a right to consent to particular uses of the information stored in the system. An exception is in FTC administrative or court proceedings, where individuals may, in some cases, limit the agency's use or disclosure of their information that may be stored in the system (e.g., pursuant to court order or in accordance with a stipulated pre-trial protective order or other binding agreement in discovery).

4.4 What are the procedures that allow individuals to gain access to their own information?

Consumers, individual defendants, and others (e.g., law enforcement contacts) do not have direct access to the information in the RED database. Individuals seeking access to such records must file a written request under the Freedom of Information Act (FOIA), 5 U.S.C. 552, with the FTC's Office of General Counsel. *See* Rule 4.11(a), 16 C.F.R. 4.11(a). Any additional request for mandatory access under the Privacy Act of 1974, 5 U.S.C. 552a, must also be made in

writing to the General Counsel, and may be filed only by an individual for records, if any, retrieved by that individual's name or other personally assigned identifier. *See* Commission Rule 4.13, 16 C.F.R. 4.13. Due to the law enforcement nature of the RED database, the General Counsel may deny access to records that are legally exempt from disclosure. *See* 16 C.F.R. 4.10(a) (nonpublic materials not subject to FOIA disclosure), 4.13(m) (Privacy Act exemptions). For information on how to file a FOIA or Privacy Act request, please visit the Commission's FOIA Web page, located at https://www.ftc.gov/about-ftc/foia.

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

There are no privacy risks associated with access to the RED system because individuals do not have access to their records within the database. Individuals seeking the RED records about themselves may only access their records as described in Section 4.4. The Commission's Privacy Act procedures permit the FTC to verify a requesting individual's identity before granting him or her access to the records at issue.

5 Web Site Privacy Issues

The RED cannot be accessed or disclosed through any public or private website. Therefore, this section is not applicable.

6 Security of Information in the System

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The RED is a part of the FTC's Data Center General Support System (Data Center GSS).[3] The FTC follows all applicable Federal Information Security Management (FISMA) requirements, ensuring the Data Center GSS is appropriately secured. The Data Center GSS is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

6.2 Has an Assessment & Authorization been completed for the system or systems supporting the program?

[3] The Data Center GSS PIA is available here: https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

Yes, as part of the Data Center GSS, an Assessment & Authorization has been completed that includes the RED.

6.3 Has a risk assessment been conducted on the system?

Yes. A risk assessment was completed for the Data Center GSS, which includes the RED.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

No.

6.5 What procedures are in place to determine which users may access the system and are they documented?

Supervisors and/or Contracting Officer's Technical Representatives (COTRs) must identify and approve employee requests to access RED and specify the appropriate level of authorization and access privileges. RED access is granted on a least-privilege-access, need-to-know basis. Access is terminated when the employee leaves the agency.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC staff are required to complete computer security and privacy awareness training annually. Interactive online training covers topics such as proper handling of sensitive PII and other data, online threats, social engineering, and the physical security of documents. Individuals with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

Auditing measures and technical safeguards are in place commensurate with the National Institute for Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53. The system is designed to ensure that users only get the information that they are entitled to access. At the database level, there are three controls: First, users must have an authorized Oracle account to access the database. Second, the database assigns roles to users to define the specific data that the user can access. Third, the roles further define what users can do with the data (i.e., read, write/edit). At the application level, RED administrators control the roles that users are assigned on a least-privilege-access, need-to-know basis to ensure that users only get the information that they are entitled to access. Further, users seeking access to RED must review and acknowledge, in writing, rules of behavior that prohibit the misuse of data. Requests

for RED access must also be approved by a user's supervisor and a RED program manager before technical staff will grant access. In addition to the controls referenced above, RED logs each individual who enters, revises, or deletes information in the system.

6.8 Where should questions regarding the security of the system be directed?

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7 Data Retention

7.1 For what period of time will data collected by this system be maintained?

Information in the RED is retained and destroyed in accordance with applicable FTC policies and procedures and with FTC Records Retention Schedule N1-122-09-1, as approved by the National Archives and Records Administration (NARA).

7.2 What are the plans for destruction or disposal of the information?

All information that is subject to disposal (see Section 7.1) will be destroyed in accordance with OMB, NIST, and NARA guidelines. Photographs used to identify defendants will be retained for no longer than 10 years, as discussed in Section 2.5.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

The FTC recognizes that there could be privacy risks associated with the disclosure of specific redress matter bank account numbers, personal information collected about defendants, including the defendants' SSNs, dates of birth, personal and employer addresses, telephone numbers, and facsimile numbers; receivers' business addresses; criminal law enforcement contacts' business addresses; and successors' and related persons' addresses and other information in the RED. The FTC further recognizes that there could be privacy risks associated with the collection, storage, and disclosure of defendants' personal information in the RED.

Such information is available to anyone with authorized, read-only access to the RED. The FTC mitigates this risk by verifying the RED's compliance with the federal and FTC-specific data security requirements established for FTC data as set forth in the FTC documentation for the Data Center General Support System. In addition, access to the RED is granted on a least-privilege access, need-to-know basis to authorized users within RAO and DE, selected employees in the FTC's Bureau of Consumer Protection and its Regional Offices, and authorized

FTC contractors performing work specifically relating to the database. Users' access rights to the RED are monitored and access is restricted or terminated when users no longer require access. Moreover, the RED logs each individual who enters, revises or deletes information from the database. All of the above individuals are bound by the FTC's Privacy Policy.

The FTC also assessed the system's "E-Survey" internal web-based tool, described in Section 1, to make sure that it was consistent with the FTC's Privacy Policy, including with regard to the use of persistent tracking technology, such as permanent "cookies" or other permanently placed software files or other information on users' computers. The internal web form associated with the "E-Survey" does not use persistent tracking technology.

All information that is subject to disposal (see Section 7.1) will be securely destroyed in accordance with OMB, NIST, and NARA guidelines.

8 Privacy Act

8.1 Will the data in the system be retrieved by a personal identifier?

Yes.

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

Yes. The applicable Privacy Act SORN is FTC I-1, which describes the FTC's Nonpublic Investigational and Other Nonpublic Legal Records, including enforcement-related data maintained by the FTC in RED, as described above. To the extent login, audit, or other data is collected and maintained about RED system users, see also SORN VII-3 -- Computer Systems User Identification and Access Records -- FTC. The SORNs are posted on the FTC's web site and can be found at http://www.ftc.gov/sites/default/files/attachments/privacy-act-systems/i-1.pdf.

9 Privacy Policy

The collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's Privacy Policy.

10 Approval and Signature Page

Prepared by the Business Owner:

_____ Date: _____
David M. Torok, Associate Director
Bureau of Consumer Protection
Division of Consumer Response and Operations

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Katherine Race Brin
Chief Privacy Officer

_____ Date: _____
Jeffery Smith
Chief Information Security Officer

_____ Date: _____
Jeffrey Nakrin
Director of Records and Filing

Approved:

_____ Date: _____
Raghav Vajjhala
Chief Information Officer