Federal Trade Commission
Privacy Impact Assessment

Redress Enforcement Database (RED)

June 2019

Reviewed February 2023

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

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 Office of Claims and Refunds (OCR) 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

OCR 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. OCR 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, OCR uses the RED to prepare cost estimates, generate work assignments, and approve administrative invoices. OCR enters 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 General Support System (GSS).[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, information from the RED system may be compared with information in the Consumer Sentinel Network (CSN) system to determine whether any relationships may exist involving likely recidivists. An automated search between the two systems is performed to determine if relevant matter-related words or individual names appear in RED that overlap with data in CSN. If a match appears, an emailed notice may be sent to the FTC staff person working on that particular matter. There is no direct connection between the two systems; for more information about CSN, refer to the Sentinel Network Services PIA.

RED limits the access rights to the administrative interface solely to OCR, 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. Finally, DE provides information from the RED to FTC data analysts who assist with the mission of enforcing judgments and orders obtained in FTC consumer protection actions.

While there is some data in the RED that relates to both missions, the interface segregates data relating solely to OCR'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-

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

privilege- access, need-to-know basis. The RED access and authorization permissions are maintained within the RED by the OCR and DE administrators.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

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 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[3] may be collected or maintained in the system/project. Check <u>all</u> that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☒ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Password
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☒ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☒ Social Security Number		
☐ Mother's Maiden Name		

[3] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

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 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.

In addition to the personal information collected about defendants (as identified above in Section 2.1), the RED may also contain 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 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.

Information about defendants from the RED is also provided to FTC data analysts who assist with the mission of enforcing judgments and orders obtained in FTC consumer protection actions by comparing that data with information from other sources available to the FTC. The information about defendants from RED provided to data analysists includes names, aliases, associates, and other information collected by the RED and described in this subsection.

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).

2.3 What is the purpose for collection of the information listed above?

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.

Division of Enforcement

DE collects the above information 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 Social Security numbers (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

OCR uses the 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 OCR performance compared to the Government Performance and Results Act.

OCR uses the RED to collect data for other offices within the FTC. OCR 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.

Historically, OCR also has tracked total dollars and checks issued by country within each matter. OCR provided data involving checks issued to consumers in foreign countries ("Foreign Claimant data") to the FTC's Office of International Affairs (OIA); this included 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). Although OCR no longer actively uses RED for these purposes, the legacy data remains in RED.[4]

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 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
Division of Enforcement Staff	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; 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. In addition, data is entered by transferring relevant data from the FTC's Matter Management System and FMO's financial system to the RED.
Office of Claims and Refunds	OCR staff enter 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 OCR based on discussions with case managers. Foreign Claimant data provided by FTC-approved redress contractors is also entered into the database by OCR staff. Finally, receiver data is entered using information from court orders and E-Surveys completed by FTC case managers.

[4] The data is stored aggregated in RED, does not contain PII, and is not sensitive. OCR is required to report on demand and they regularly receive requests about this data from OIA. The data is kept to support the OCR mission.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Note: No external entities have direct access to the RED system. OCR or DE may extract data or reports from the RED to provide to external entities as described in the chart below.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
Authorized FTC staff	The RED may be accessed by case managers, OCR and DE staff, other authorized FTC staff in BCP or the FTC's Regional Offices, as well as 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 OCR/DE administrators, OCR/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 OCR 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 OCR/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.
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

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	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.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

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 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

All FTC contractors who have access to the RED system adhere to the same privacy and security guidelines and policies that FTC employees must follow. In case of a privacy incident, they must follow the procedures detailed in the FTC Breach Notification Response Plan. External redress contractors do not have access to the RED system.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☐ Notice is not provided (explain):_____
☒ Notice is provided via (*check all that apply*):
- ☐ Privacy Act Statement (☐ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*):

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. Where applicable, the FTC may also provide a Privacy Act statement on information collection forms used to collect information to be maintained in an FTC Privacy Act records system.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

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.

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).

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Consumers, individual defendants, and others (e.g., law enforcement contacts) do not have direct access to the information in the RED. 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/foia.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As stated in 4.3, Consumers, individual defendants, and others (e.g., law enforcement contacts) do not have direct access to the information in the RED. 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. Individuals may file requests with the FTC under the FOIA and the Privacy Act of 1974 for access to any agency records that may be about them and are not exempt from disclosure to them under those laws. Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

When BCP case managers reply to an E-Survey, the information is reviewed by administrators, supervisors, and/or program staff in DE and/or OCR. When all the necessary data elements are provided, OCR and DE enter the data into the RED. If information is missing from an E-Survey, DE or OCR 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. OCR 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. OCR 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 OCR annually. Photographs identifying individual defendants, when included in a matter, are retained in the RED for 10 years and then automatically purged from the system.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the National Institute for Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations 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 the 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.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

The data made available to the contractor in the development and test environments is scrubbed and scrambled to remove any resemblance to live production data. Sensitive data elements are scrambled using an algorithm that renders it infeasible to convert that information back to the original data.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

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). All information that is subject to disposal 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.[5]

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

The FTC utilizes the RED system's web-based "E-Survey" tool, which is only available internally to the FTC. The "E-Survey" 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. The internal web form associated with the "E-Survey" does not use persistent tracking technology.

8 Privacy Risks and Evaluation

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

Risk	***Mitigation Strategy***
Individuals who have access to PII could exceed their authority and use the data for unofficial/malicious purposes	The RED administrators in DE and OCR 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. The RED interface segregates the data relating solely to OCR's mission from data that relates solely to DE's mission. Access to either organization's data is provided by that organization to

[5] DE stores defendant photographs in RED in order to: (1) identify defendants (DE often inherits cases where they have had no prior dealings with defendants and therefore needs photos to spot defendants appearing in promotional materials, which facilitates compliance review); (2) identify defendants to receivers when needed; (3) obtain consumer identification of defendants; and (4) help effectuate service. Storing the photos also eases DE's efforts of finding photos in old, voluminous files and reduces the number of requests to other staff for those materials. Photos over 10 years old are purged from the system to keep the photos current and manage the quantity of images maintained. The retention period is longer than the redress period because defendants are often bound by permanent injunctive relief as to their commercial activities.

Risk	*Mitigation Strategy*
	authorized users on a least-privileged access, need-to-know basis. These restrictions help to protect the information in the RED from internal threats.
Unauthorized access to information in RED	Only FTC staff and contractors with an OCIO-issued user-identification and strong password can access the FTC network where the RED is housed. The server on which the RED 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. These controls help protect RED from unauthorized access.
Disclosure of specific redress information	The FTC recognizes that there may be privacy risks associated with the disclosure of certain redress information, such as bank account numbers, personal information collected from defendants (including SSNs, dates of birth, personal and employer address, telephone or fax numbers), business 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. The FTC mitigates these risks by verifying the RED's compliance with the federal and FTC-specific data security requirements established for the FTC GSS. In addition, access to the RED is granted on a least-privilege access, need-to-know basis to authorized users within OCR and DE, selected employees in the FTC's Bureau of Consumer Protection and its Regional Offices, and authorized contractors performing work specifically relating to the database. Users' access rights to the RED are monitored; 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. The FTC also assesses the system's "E-Survey" internal web-based tool 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 on users' computers. The internal web form associated with the "E-Survey" does not use persistent tracking technology.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

The system uses several controls to enhance and support privacy. The system automatically locks out after three unsuccessful login attempts, which requires the user to unlock the account by contacting FTC OCIO and providing valid credentials. Additionally, the system automatically records the login/logout details of the user along with the machine used to log on to track access. Within the application, SSN/DOB/EIN data is shown in a separate window that does not contain other details; in other words, additional PII data fields like name, address, are not shown within the same window.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

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. 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. All FTC SORNs are available online.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

Legal and technical controls are in place to ensure that information in the RED is collected, used, stored, and disseminated in accord with the provisions of this PIA.

With respect to legal controls, as a general matter, staff may not disclose nonpublic agency information, including that stored in the RED. Unauthorized disclosure of nonpublic information submitted to the Commission is subject to criminal prosecution and punishable by fines or imprisonment under the FTC Act, 15 U.S.C. § 50. Under certain circumstances, unauthorized disclosure of nonpublic agency information is subject to criminal sanction under the Trade Secrets Act, 18 U.S.C. § 1905, the Larceny Act, 18 U.S.C. § 641, and SEC Rule 10b-5. Disclosures of nonpublic information may result in disciplinary action. However, disclosure of nonpublic agency information may be permissible in circumstances defined by statute or FTC rule.

As to technical controls, as described more fully above, the RED employs a design that focuses on the safeguarding of data. Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the NIST Security and Privacy Controls for Federal Information Systems and Organizations 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 described in section 5.2, above. In addition to the controls referenced above, the RED logs each individual who enters, revises, or deletes information in the system.

The RED is housed within the FTC GSS. The FTC follows all applicable FISMA requirements, ensuring the GSS is appropriately secured.