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

☒	☐	☒
☒		☐
☒	☐	
☒	☒	☒
☐		
☐	☐	☒
☐		
☐	☐	
☐		
☒		
☐	☐	
☐		
☐	☐	
☒		
☐		
☐	☐	

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.

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

3 Data Access and Sharing

3.1

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

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)

☐

Individuals

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. iTh(e)]TJ3 The .w 3 Tr 0.78 0 Td(chmTw [(t)fM[(s)ss

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*
	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/