

Redress and Enforcement Database
Privacy Impact Assessment

June 2007

INTRODUCTION

To further its consumer redress and law enforcement missions, the Federal Trade Commission's (FTC) Redress Administration Office (RAO) and Division of Enforcement (DE) collect and maintain certain personal information concerning defendants against whom the FTC has obtained judgments and/or injunctive orders in judicial or administrative proceedings for violations of the FTC Act and other statutes and rules enforced by the FTC. The personal information collected includes defendants' names, addresses, social security numbers (SSNs), employer identification numbers (EINs), the names and addresses of defendants' attorneys, agents, associates, employers, successors, as well as information relating to the date, type, and amount of the orders or judgments obtained. The information enables the Commission to monitor compliance with injunctive orders, collect outstanding judgments, and return the maximum amount possible to victimized consumers.

The RAO originally collected some of this information in a single-user database application created in 1996. This prior database was not user-friendly, required manual entry of all data elements, and became unusable in August 2004. Additionally, in 2005, DE decided to develop a database to support its mission of enforcing federal court and administrative orders. Accordingly, the RAO and DE, jointly working with the Office of Information and Technology Management (OITM) and with contractors, have created a Redress and Enforcement Database System (RED) to replace the existing redress database. The new database will automate the RAO's oversight of the FTC's redress contractors as much as possible, and streamline DE's recordkeeping with respect to persons subject to FTC orders, thereby assisting the FTC in enforcing those orders and returning funds to victimized consumers.

RED utilizes the Oracle Relational Database Management System as the data repository, data security and integrity engine, and business rules engine. Using Oracle maximizes data quality, data security, and system performance. Users access RED using one of two graphical user interfaces – one web-based and one developed using Microsoft Access. RED minimizes the manual keying and re-keying of relevant data by having the case managers enter the data via an electronic, web-based questionnaire ("E-Survey") instead of on a handwritten form, and by transferring relevant data from existing FTC systems, including the Matter Management System (MMS) and the Federal Finance System (FFS). RED maximizes data security by restricting the ability to view the E-Survey for a particular case to the case manager assigned to that case and limiting rights to the Microsoft Access interface to RAO and DE staff and those FTC users authorized by such staff. Users have the ability to read or modify data only if they have been specifically granted such rights for business purposes. While there is some data that relates to both missions, the Microsoft Access interface further maximizes data security by segregating any 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 with a need to know for official business.

In addition to data concerning defendants, orders, and judgments, RED will collect other information that will further the FTC's order enforcement mission. First, to assist staff in ensuring defendants' compliance with permanent injunctions, RED will track whether defendants have timely submitted all required compliance reports and identify defendants whose compliance monitoring provisions may be expiring. Second, RED will contain contact information for the defendants' attorneys, agents, employers, successors, and associates who may have information about the defendants' activities or who may be the subject of future law enforcement action. Successors and associates are entities who may be required by law to comply with an order obtained by the FTC, either as successors-in-interest and/or pursuant to Federal Rule of Civil Procedure 65. Third, RED will include contact information for criminal law enforcement authorities and receivers. Therefore, RED also will serve as a resource for staff in identifying potential targets, other law enforcement staff receptive to criminally investigating our targets and defendants, and potential receivers.

As explained below, the FTC has taken steps to mitigate the privacy risks associated with the information collected by this new system.

SYSTEM OVERVIEW

RED replaces the existing redress database system, which relied upon manual entry of data gathered by distributing paper questionnaires to individual FTC staff attorneys who completed them by hand. RED will gather the same information by periodically sending FTC staff attorneys the "E-survey," an e-mail containing a link to a web-based questionnaire to be filled out on their computer desktop.

ANALYSIS

1. The Information That Will Be Collected (Nature and Source)

The previous redress information system compiled and maintained personal information such as a defendant's name, SSN or EIN, date of birth, address, home and work telephone phone number, and e-mail address, as well as details regarding the defendant's employment. RED also compiled and maintained information about the amount of the judgment debt, the date the judgment becomes due, payments, debt delinquency or default, and amounts accrued for interest, as well as the duration of recordkeeping and compliance monitoring requirements set forth in an order, and the status of order compliance cases. Neither the old nor the new database has ever maintained personal information regarding consumers. Neither do these systems document consumer activity such as the purchasing of products or services.

The FTC collects the personal information regarding defendants directly from the individuals and businesses who are the targets of FTC law enforcement actions and also from financial statements that defendants may be required to produce. In addition, the FTC may receive personal information in the course of an investigation, in litigation, or in the context of

settlement negotiations. The FTC also may obtain information from credit bureaus, publicly available databases (such as Lexis/Nexis), or federal, state, or local agencies furnishing identifying information.

To implement RED, the FTC determined that several additional, broad categories of information concerning redress distributions should be compiled and maintained. For example, the new system will compile and maintain information concerning the number of redress distributions, the 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. However, the new system will not contain specific information regarding the terms of redress distribution to individual consumers.

Finally, both the old database and RED contain contact information for receivers appointed in particular cases as well as criminal law enforcement authorities that might be involved in parallel investigations or prosecutions. In addition, RED will for the first time include contact information for defendants' attorneys, agents, successors, and associates, who may have information about the defendants' activities or who may be bound by a prior order or the subject of future law enforcement action. This information consists of name, address, and telephone and facsimile numbers.

2. Why The Information Is Being Collected

The FTC 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 fulfill its responsibilities to enforce existing injunctive orders and collect on its judgment debts to distribute monies to injured consumers. This information is also collected to facilitate the collection and resolution of debts delinquent more than 180 days through the Integrated FedDebt Program (FedDebt) of the Department of the Treasury's Financial Management Service (FMS). 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 all judgments no longer being litigated that have been outstanding and delinquent for 180 days or more to the Department of Treasury for collection. The Treasury requires the FTC to provide each judgment debtors' name and SSN or EIN.

Additionally, the FTC must collect SSNs and EINs in connection with tax reporting requirements for judgment defendants. If a debt referred to Treasury is not collectible, Treasury will issue 1099-C forms to each defendant who has not paid an outstanding judgment in full.

Furthermore, the FTC collects address information for receivers and criminal law enforcement authorities to assist staff in prosecuting their existing cases. As previously noted, the FTC also collects address information for defendants' successors and associates in order to maintain a record of persons or entities who may have information about the defendants' 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.

3. The Opportunities Individuals Will Have To Decline To Provide Information or To Consent To Particular Uses of Information and How Defendants Grant Consent

As previously discussed, the FTC's and Treasury's MOU under the DCIA requires the FTC to send all delinquent judgments no longer in litigation to the Treasury for collection after 180 days. In furtherance of collection, the Treasury requires the FTC to provide SSNs, EINs, and other identifying information regarding these judgment debtors. To the extent the FTC attempts to collect this information directly from defendants through investigation, litigation, or voluntary settlement negotiations, defendants have notice of the FTC's efforts and 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 request 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 from third parties and other sources, such as other law enforcement agencies or private credit reporting agencies, or public sources, defendants may not necessarily have notice or an opportunity to consent to the collection or use of the information.

The FTC also may attempt to obtain personal information concerning defendants' employers, attorneys, agents, successors, and associates whose information will be collected in the database through discovery in litigation or from publicly available sources. To the extent the FTC collects this information directly from the persons or entities in question, or attempts to do

so, whether through investigation, litigation, or voluntary negotiations, those persons or entities have notice of the FTC's efforts and opportunity to decline cooperation or to assert a privilege or immunity from providing this information. However, some of these entities may not have notice or an opportunity to consent to the collection and use of their information.

With respect to the contact information collected for receivers and criminal law enforcement authorities, such information is widely publicly available. Thus, although such persons are not given an opportunity to consent to the collection of their contact information or its use in RED, there is no associated privacy impact.

4. Intended Uses of the Information Collected

The FTC will use information in RED to administer its order enforcement activities and collect monies from defendants who have defrauded or otherwise victimized consumers and who have been prosecuted through an FTC law enforcement action. The FTC may also use the information about defendants, and their agents, successors, and associates, to pursue corollary investigations, to meet tax reporting obligations, and for any other uses authorized by existing Privacy Act System of Records notices, as discussed more fully in section seven.

The FTC will use 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 will use the contact information of criminal law enforcement personnel to identify interested law enforcement authorities and to prosecute existing FTC cases.

5. With Whom the Information Will Be Shared (Disclosures)

The FTC uses and shares information collected by RED to further its consumer protection and redress mission. The use of data in RED is in accordance with routine uses outlined in the FTC's Privacy Policy and the Privacy Act System of Records Notice.¹

FTC Staff and Contractors

Authorized FTC staff within RAO and DE and selected employees in the FTC's Bureau of Consumer Protection and its Regional Offices may use information in RED to store and review data relating to FTC law enforcement actions and to collect monies from defendants who have been prosecuted in such actions. In addition, RED data is used to assist with periodic reviews of the effectiveness of the FTC's order enforcement program and its consumer redress procedures. Aggregate numbers developed from RED data may also help determine the effectiveness of the FTC's redress collection and distribution procedures.

¹ For FTC's Privacy Policy, see <http://www.ftc.gov/ftc/privacy.htm>. For the Privacy Act System of Records notice, see 57 Fed. Reg. 45,678 (Oct. 2, 1992), <http://www.ftc.gov/foia/listofpaysystems.shtm>.

A limited number of authorized FTC contractors may access data in RED to perform technical work relating to the development and maintenance of the system. The contractors are bound by non-disclosure agreements prohibiting unauthorized disclosure of information collected by the agency.

The Department of Treasury

The FTC discloses data collected in RED to the Treasury when it refers eligible defendants to the Treasury for further collection of judgments. Treasury may share this information with the Department of Justice or any of the private collection agencies that may be assigned the FTC debt for collection activities. These disclosures are appropriate because monies ultimately collected by Treasury, DOJ, or private collection agencies will be used (if appropriate) for consumer redress. If a debt proves to be uncollectible, Treasury will then issue 1099-C forms to each defendant who has not paid a judgment in full.

External Law Enforcement

The FTC may disclose information collected in RED with other federal, state, local, or international law enforcement agencies in the course of a law enforcement investigation or action. These disclosures are appropriate to further the FTC's consumer protection mission.

Other Disclosures

The FTC may be required or authorized to share certain data collected in RED in other circumstances, including in response to requests from Congress, Freedom of Information Act (FOIA) requests from private individuals or entities, 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.

6. Security (Administrative and Technological Controls, Including Maintenance and Disposal)

The FTC follows all applicable information technology requirements and procedures required by federal law and policy to ensure that information in RED is appropriately secured. RED is a Major Application that rides on the infrastructure of the General Support System and poses a moderate security risk. Consistent with agency requirements under the Federal Information Security Management Act, the FTC has undertaken a formal certification and accreditation process to ensure that the information in RED is appropriately secured in light of

for any security questions relating to RED. With respect to the certification and accreditation of RED, Stanley Lowe shall be the Designated Approving Authority.

The FTC also takes appropriate steps to ensure that defendants' data is protected and safeguarded against interception when it leaves RED and is sent to Treasury. Using the Treasury's FedDebt Program, the FTC transmits all debt referrals electronically, through Treasury's secure, web-based system. The Commission retains any Treasury correspondence for at least a year, and may retain automated information indefinitely, subject to earlier deletion, as authorized.

7. Privacy Act

The information concerning defendants, associated persons, and receivers to be collected in RED is covered by an existing Privacy Act System of Records notice, which describes, in particular, System FTC I-1: Investigational, Legal, and Public Records. The categories of individuals covered by that system include, *inter alia*, "Participants in Commission . . . law enforcement proceedings. . . ." The categories of records in the system include, *inter alia*, "Name, address, employment status, age, date of birth, financial information, credit information, personal history, and records generated and collected through the investigation. . . ." *See generally*, 57 Fed. Reg. 45,678 (October 2, 1992). The system therefore does not require a new Privacy Act System of Records notice.

As elaborated in Section 3, above, defendants, associated persons, and receivers are, under certain limited circumstances, given notice of the collection of such information and an opportunity to consent.

8. Other Privacy Considerations and Analysis

The collection, use, and disclosure of information in this system has been reviewed to ensure that the agency's practices are consistent with the privacy policy that the Commission is required to post on its Web site pursuant to the E-Government Act of 2002, Pub. L. No. 107-347, and OMB implementing guidance (M-03-22, Sept. 26, 2003). The Commission's Privacy Policy can be accessed on the FTC web site at the following URL: <http://www.ftc.gov/ftc/privacy.htm>.

The FTC identified the potential risks of collecting personal information in RED, particularly SSNs and EINs, and took steps to mitigate those risks. First, the FTC chose to limit

procedures required by federal law and policy to ensure that information in RED is appropriately secured, (ii) has conducted a risk assessment, identified appropriate security controls to protect against assessed risks, and implemented those controls, (iii) will monitor, test, and evaluate RED on a regular basis to ensure that those controls continue to work properly, safeguarding information, and (iv) provided the appropriate point of contact for any additional questions from users.

the type of information to be maintained and collected by this system. Particularly, the FTC limited the database to essential information concerning defendants and associated persons, the injunctive provisions potentially applicable to them, and the monetary relief obtained against defendants. The FTC did not include in the database personal information from victimized consumer. Second, to the extent the FTC collects defendants' SSNs and EINs, they are encrypted such that users with read-only access and outside hackers will not be able to see them; only authorized FTC staff will be able to view this information.

Additionally, the FTC recognizes that there could be privacy risks associated with the disclosure of addresses, telephone numbers and facsimile numbers in RED. These include the defendants' personal and employer addresses, receivers' business addresses, criminal law enforcement contacts' business addresses, and successors' and related person's addresses. Such information is available to anyone with read-only access to the system. However, the level of protection for this information is consistent with data protections afforded for similar information by other data systems maintained by the FTC, notably the MMS and Consumer Information System (CIS). Moreover, unlike CIS, access to RED will be limited to FTC employees and contractors, who are bound by the FTC's Privacy Policy. Access to RED is restricted 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.

The FTC also assessed the system's "E-survey" web form for privacy risks associated with the use of persistent tracking technology, such as permanent "cookies" or other permanently placed software files or other information on user's computers. Because the web form activated by the "E-survey" does not use such persistent tracking technology, no such privacy risks are raised. Similarly, the FTC assessed whether RED posed a risk to interests protected by the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq.* Because RED data entry rights are available only to authorized FTC staff, and because RED is not available on the Internet, no risks associated with the on-line collection, use, or disclosure of personally identifiable information related to children are raised.