Federal Trade Commission
Privacy Impact Assessment

for the: BCP Redress Program

1 System Overview

The Federal Trade Commission's Bureau of Consumer Protection (BCP) litigates cases that often result in the award of redress money that is to be returned to affected class members (either injured consumers or businesses.) Disbursement of money in the redress fund is made pursuant to a distribution plan either approved by the court or the administrative law judge or delegated to the FTC's discretion. The Redress Administration Office (RAO) is responsible for administering and coordinating redress activities. Four redress contractors (Analytics, Inc., Gilardi & Co., LLC, Rust Consulting, and Epiq Systems) have been awarded a contract supporting RAO's goals. Each contractor stores consumer and business data, received from RAO, in proprietary databases supported by a Microsoft SQL back-end and a web-based front-end, for the purpose of meeting contractual obligations to:

- operate efficient and cost effective claims administration, which permits redress class members world-wide to receive monetary disbursement from defendant-funded settlements or litigated final orders;

- provide the FTC access to matter-specific class member and financial transaction information through standard and ad hoc reports; and

- provide injured class members and other consumers with easily accessible points of contact through consistent, timely and professional telephone and written responses to their inquiries.

The contractors maintain physical systems (servers, routers, SAN, etc…) in their secure on-site and off-site locations.

2 Information Collected and Stored within the System

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

The class member data collected, used, disseminated or maintained either within RAO or within the redress contractors' proprietary databases varies depending upon the redress matter. In routine cases the following information is used: first and last name, business name (if needed), street address, city, state, postal code, country, home phone number, work phone number, email address, transaction data, transaction dates, product type, company selling product, customer number, customer account number, and loss amount. In rare instances, Social Security numbers or Tax ID numbers, credit card numbers, bank account numbers, and bank names may also be collected and used.

.2 **What are the sources of the information in the system?**

Class member data is received from three primary sources:

- initial source data found in defendants' files and consumer complaints submitted to the FTC;
- address corrections provided by third party data sources such as the United States Postal Service (USPS) and Lexis/Nexis; and
- data provided directly by class members as part of the redress administration process.

.3 **Why is the information being collected, used, disseminated, or maintained?**

Information on either consumers or businesses is collected, used, disseminated, or maintained by RAO staff and redress contractors in order to make redress payments to appropriate class members. In the typical case, only the following minimal amount of information is used:

- Consumer Name or Business Name;
- Street Address; and
- Class member loss amount.

In some instances RAO may provide to the contractor, as an identifier, class members home telephone number, work telephone number, email address, transaction data and dates, product type, company selling product, and customer account number.

On rare occasions redress refunds may create a tax implication for class members. These very infrequent instances necessitate the RAO to collect and disseminate SSNs and EINs to the redress contractor. The contractor uses the SSNs and EINs to prepare tax forms which are mailed to the injured class member and electronically reported to the IRS over a secure Federal government network. Furthermore, bank account or credit card numbers are rarely collected, maintained and used; and if so, only when no other identifier is available.

Prior to maintaining and disseminating data, RAO staff removes all unnecessary information from the data file and only forwards encrypted data to redress contractors.

.4 **How is the information collected?**

Consumer information may be collected directly from defendants' files. The FTC also gathers consumer complaints that have been submitted either directly to the FTC or to another organization that shares its complaints with the FTC. Supplemental information is collected either by third party sources in the form of address corrections, or directly from potential class members in the form of completed claim forms, correspondence, or telephone calls. Correspondence from individuals is received via fax submissions, web based data collection, and electronic transmission.

.5 **How will the information be checked for accuracy and timeliness (currency)?**

Various steps are taken to validate the accuracy and timeliness of collected data based on its original source. For example, prior to the contractor mailing a claim form, redress check or consumer education material, class member addresses are standardized and validated against known data sources, such as the USPS National Change of Address Database and postal service records regarding street names and address ranges. All additions, deletions and address changes to the data set are approved by the RAO and reconciled against the original source data.

In many instances, claimant data is obtained from defendants' files, and that data is used to mail redress checks directly to injured class members. In other cases, claim forms are mailed to a known set of class members requesting that they validate, under penalty of perjury, their address, loss amount and entitlement to redress. In other cases, claim forms will be made available to previously unknown class members via a case specific redress notification outreach effort. Again, class members record their address, injury amount and entitlement to redress under penalty of perjury.

All check distributions and claim form responses are reviewed by the redress contractor to confirm that the loss amounts claimed are consistent with a set of established case specific parameters. Outreach material, redress checks and claim forms always include a telephone number and mailing address for consumers to contact the contractor to have their questions answered and/or to update their information.

.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.

.7 **What law or regulation permits the collection of this information?**

No law or regulation specifically permits the collection of this information. The FTC collects this information in order to provide redress to injured class members as part of our law enforcement activities carried out pursuant to the FTC Act and other statutes.

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

In the vast majority of redress matters, the information stored by RAO and the redress contractors is identical to publicly available information about consumers. The only exceptions are when the contractors:

1) collect information relating to individual transactions; or
2) collect information required by the IRS for tax reporting.

As discussed later in this document, comprehensive data security plans have been implemented to protect this data, including frequent, automated scans of information systems as well as policies and procedures to limit access to sensitive data and ensure compliance with data

privacy standards.

3 Use and Access to Data in the System

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

The information in the system will be used to calculate and distribute individual class member redress payments and/or consumer information. This effort may include a combination of printing and mailing claim forms, processing claims and corrections submitted by class members, issuing checks or other forms of payment, and/or providing consumer education.

Data in the system will be accessed by contractor staff to determine class member redress eligibility. The data will be accessed via secure login at the user level and only made available to authorized staff on a need-to-know basis. Data usage is in accordance with routine uses outlined in the redress contract.

.2 Which internal entities will have access to the information?

RAO staff has access to the information, as well as the following approved redress contractor staff:

- Information Technology professionals, for the purpose of importing, validating, updating and storing class member data;
- Claims processors, for the purpose of validating eligibility, communicating with class members, and updating their contact information; and
- Management, for the purpose of supervising technology and processor resources and ensuring accuracy and adherence to data handling standards.

RAO staff along with contractor staff with access to class member information have completed
non-disclosure forms, fingerprints and personal information for FTC background checks and clearance.

.3 Which external entities will have access to the information?

In some redress distributions, consumer name, address and redress amount information is encrypted using PgP and transmitted to authorized sub-contractors for assisting in the printing and mailing process. On occasion, the encrypted information may also be shared with law enforcement and other government agencies, courts, and defendants, or as otherwise authorized by the law.

4 Notice and Access for Individuals

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

Redress cases which necessitate contractor collection of class member information via a claim form always include a Privacy Act Notice. In certain cases, class members may submit claim

forms online via a secure website, which will also contain a Privacy Act Notice.

As for information provided to the redress contractors by the FTC, if the information was obtained from class member complaints personally submitted to the FTC, then those class members received a similar Privacy Act Notice via the FTC online complaint form or telephone system. If the information was obtained solely from defendants, class members did not receive this notice. All class members receiving a Privacy Act Notice are provided a mailing address and telephone number to update and provide additional information about their status. In addition, as previously mentioned in section 2.5, all redress checks also include a mailing address and/or telephone number to allow consumers to contact the redress contractors concerning their information.

.2 **Do individuals have the opportunity and/or right to decline to provide information?**

Individuals who receive a Privacy Act Notice are informed that they have the right to refuse to provide information and the associated consequences.

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

Consumers do not have the right to consent to particular uses of their information. They consent to their information being provided for all uses described in the applicable privacy policies. The consumer exercises these rights by choosing to complete, sign and submit a claim form.

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

Class members can access their information by contacting the redress contractor. Before making any class member requested changes to their information, the contractor will confirm the class member's identity by asking a series of questions and instructing the class member to forward their change request in writing along with supporting documentation if needed. Contractors accept written documentation via fax, mail or email. Otherwise, individuals may gain access to their own information through a Privacy Act request.

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

Information will not be provided to individuals that have not been named as a class member, unless proof of authority to receive information has been filed in writing. Minimal if any risks to individuals exist in accessing their own information.

5 Web Site Privacy Issues

.1 **Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for**

use by the FTC (see 5.2).

The redress contractors' websites do not use tracking technology.

.2 If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

Not Applicable.

.3 **If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.**

Contractors use as a minimum 128-bit SSL encryption when personal information is collected through a web site, page, or online form.

.4 **Explain how the public will be notified of the Privacy Policy.**

The Privacy Policy set forth in section 4.1 is posted on all redress case specific websites developed and hosted by redress contractors' and on all online claim forms.

.5 **Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.**

Redress contractors have identified privacy risks associated with their redress websites and have taken steps to mitigate those risks. The following privacy risks were identified:

- When submitting a claim form, a class member might inadvertently provide sensitive PII information that may not be required, which poses a risk of identity theft;
- Data provided by individuals might not be accurate, complete, or timely; and
- Data provided by class members might be misused or improperly disclosed or accessed.

To mitigate the risk of unnecessary PII (Personal Identifying Information) being provided by class members, the claim forms do not include a comments field. Furthermore, fields are limited to essential information to process a claim, reducing the risks of a user accidentally providing unnecessary information. Social Security numbers are not collected on claim forms.

As to the risk that the data provided might not be accurate, complete, or timely, it is important to note that individuals voluntarily provide claim information on the website, so that they may receive redress. The process of filing claims is made as easy as possible for individuals. Class members retain the right to update any inaccurate information by the procedures detailed in section 4.4.

To mitigate the risk of the use and disclosure of consumer data, the contractors employ a significant number of layered technical controls to help prevent the misuse or improper disclosure or access to consumer data.

.6 **If the Web site will collect personal information from children under 13, or**

be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

Not Applicable.

6 Security of Information in the System

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

Yes, each redress contractor employs both information security and physical security to the privacy related information it collects. The contractors have received Federal Information Security Management Act ("FISMA", 44 U.S.C. § 3541, et seq.) and National Institute of Standards and Technology (NIST) certification as a mission-critical, moderate-security system. Contractor systems are routinely reviewed and audited by the FTC to ensure compliance with FISMA and NIST.

.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

Yes.

.3 Has a risk assessment been conducted on the system?

Yes.

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

No, the technology employed by the redress contractors does not raise any special privacy concerns not already addressed.

World Wide Web (HTTP) technology is used by each contractor within a closed network that is not accessible outside of their facility. To ensure the privacy of the data, the systems use Secure Socket Layer (SSL) encryption between the server and each user. Each user must use a secure password to gain access to the system as a whole, and then only users authorized to work on a particular redress matter have access to that matter's data.

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

Each redress contractor limits electronic access to their database to authorized users who are furnished with appropriate user rights, which are granted only to the minimum extent needed to fulfill job functions.

Account management policies and controls are in place to manage system accounts, to include the establishment, activation, modification and termination of system accounts. Employee Modification Forms are used to obtain information to establish user accounts. Security verifies that the individual meets all the requirements outlined in the policy for access to

the system. The IT staff then creates the end-user's account in Active Directory (AD) and once the AD account is created, the end-user is assigned a role in the application via their AD account. The contractors systems use role based access controls that provide only the necessary functions to users such as the need to view, add, and change data in the system. The account management policies are defined in the IT Security Policies and the procedures are documented.

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

Each redress contractor requires authorized users to be trained in the contractor's privacy policy and agrees to maintain class member and company information in the strictest privacy. This training and agreement is renewed annually and following any policy change**.**

All FTC employees are required to complete an IT Computer Security and Privacy Awareness Training annually. This interactive online training module covers topics such as how to properly handle sensitive PII and other data, online threats, social engineering, and the physical security of documents. In addition, all FTC staff is required to complete a Mandatory Compliance Checklist for sensitive PII and SHI. Furthermore, persons at the FTC with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

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

Each redress contractor limits users' access to data based on their role. All privileged users are required to login with a valid user ID and password. No actions can be performed on the contractor systems without identification or authentication. Systems and processes are periodically reviewed by system owners and the FTC.

.8 State that any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

Any questions regarding the security of the redress contractors' systems will be directed to the FTC's Chief Information Security Officer, Margaret Mech, at (202) 326-2609.

7 Data Retention

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

Electronic data collected is maintained for six years.

.2 **What are the plans for destruction or disposal of the information?**

All disposal of information is conducted in accordance Office of Management and Budget (OMB) and NIST guidelines.

.3 **Describe any privacy risks identified in the data retention and disposal of the**

information, and describe how these risks have been mitigated.

Data is stored in working systems behind multiple redundant layers of physical and electronic access control to mitigate risks of unauthorized access or sabotage. Encryption technology is employed.

8 Privacy Act

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

Yes, the data stored by the redress contractors can be retrieved by the following personal identifiers:

- Consumer Name or Business Name
- Street Address
- EIN or SSN
- Telephone Number
- Email Address
- Unique FTC Reference Number

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

Yes, the redress contractor databases are covered by an existing Privacy Act System of Records notice FTC-I-1, which can be viewed online at, http://www.ftc.gov/foia/listofpaysystems.shtm

9 Privacy Policy

.1 Confirm that the collection, use, and disclosure of the information in this system have been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of the information in the proprietary contractor systems have been reviewed to ensure consistency with the FTC's privacy policy.

10 Approval and Signature Page

Prepared for the Business Owners of the System by: