Federal Trade Commission
Privacy Impact Assessment

for the: Rust Consulting Online Claim Submission Websites

January 9, 2012

Rust Consulting Online Claim Submission Websites
Privacy Impact Assessment

Executive Summary

The Federal Trade Commission's ("FTC") 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, including Rust, have been awarded contracts supporting RAO's goals. In 2008, a comprehensive Privacy Impact Assessment ("PIA") was conducted for the BCP Redress Program and is available at http://www.ftc.gov/os/2008/09/0809bcpredresspia.pdf (Redress Program PIA). The Redress Program PIA details the protections in place to store consumer and business data from RAO in proprietary databases managed individually by the each of four approved redress vendors.

This PIA (Rust Online Claim Submission Websites) addresses specific issues raised by the Online Claim Submission ("OCS") websites administered by redress contractor Rust, and it supplements the Redress Program PIA and should be read in conjunction. Only those sections of the Redress Program PIA directly affected by these new issues are addressed in this PIA (Sections 1, 4, 5, and parts of 2 and 6).

Rust will use its OCS website to provide individuals with the ability to submit claims electronically.

1 System Overview

The OCS websites are hosted on a network accredited under the Federal Information Security Management Act ("FISMA") (44 U.S.C. § 3541 et seq.) and employ processes and technologies covered in the Redress Program PIA. The FISMA-accredited network provides security for stored and transmitted data through the use of process and technology controls. Access to OCS websites will be through the FTC website. The FTC website will display the FTC's privacy policy, which generally describes how the FTC uses and maintains information it collects. The FTC website will also display specific FTC Privacy Act statements for OCS sites, where claims data is actually submitted and collected electronically from individuals.

OCS websites allow claimants in redress cases assigned to Rust to submit claims electronically. Each redress case that includes a claim process may have a separate OCS website that can be branded accordingly.

To access the OCS website, claimants will follow an authentication process. Claimants will receive a unique claim identifier via claim form that is mailed or emailed to them. (Possible identifiers include a claim number and temporary password or another known shared data element such as an account number or zip code, etc.). Claimants visit the OCS website and enter their unique claim identifier information and an email address. New authentication credentials will then be generated and sent to the email address provided.

This new set of authentication credentials (email address and password) will allow a claimant to access the account established for him or her to submit claims data through the OCS website. At this point, the temporary information printed on the notice can no longer be used to access the account. This authentication process serves as a deterrent to fraud as email addresses can be tracked, if required (i.e., the address is a record of what e-mail account was used to access the account). Once claimants' accounts have been established and authenticated in the case-specific OCS website, claimants will be able to enter, review, or edit their information before the claim is formally submitted and accepted by Rust for processing. Once a claim form is formally submitted and accepted by Rust, edits can only be made by contacting Rust via telephone, using the number found on the website.

After users enter appropriate data and continue to the next screen, which is the final step before data is saved, Captcha validation is required. Captcha is a web standard for verifying human input and preventing automated form completion.

When data is saved, a confirmation number is displayed to the user for their records. Potential claimants can utilize that confirmation number to call and check the status of their claim.

If a claimant chooses not to submit a claim form online, the claimant can download a claim form and mail or fax it in.

Rust also has an option for online claim filing on a per-case basis where individuals who were not mailed a notice believe they are entitled to file a claim as they learned about the redress case by other means. These claimants can access the OCS websites and submit their email information to receive authentication credentials as described above.

2 Information Collected and Stored within the System

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

The OCS site will collect and maintain specific information about individuals and their claims, depending upon the redress matter. In routine cases, in addition to the individual's login data (identifier and password), the site will ordinarily collect: 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.

In addition, OCS websites collect standard web log information in an effort to prevent fraud, improve website quality, and assess the overall utility of the service, including whether claimants are using the service. Information collected by OCS websites also includes the user's IP (internet protocol) address, the referring IP address or domain (the prior website visited), date and time of the visit, pages visited, and pages requested. Rust cannot directly correlate the data collected to identify specific users.

4 Notice and Access for Individuals

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

Individuals are informed about what information the FTC collects from individuals and others and how it is used, through the FTC's Privacy Policy (ftc.gov/ftc/privacy.shtm), which will be linked on the OCS websites. In addition, the FTC will provide Privacy Act statements (see sample below) on the printed notice sent to claimants and at the appropriate location on the OCS websites where login or claims data is actually collected from individuals. The Privacy Act statement informs individuals about what information is collected and how this information may be used and disclosed.

FTC PRIVACY ACT STATEMENT – OCS

The information requested on the Claim Form is being collected in order to make a distribution of funds paid to the Federal Trade Commission pursuant to a judgment resolving allegations of unfair and deceptive acts and practices in or affecting commerce, pursuant to 15 U.S.C. § 45(a). In addition, the information may be disclosed for other purposes authorized by the Privacy Act, 5 U.S.C. § 552a, as described in the applicable FTC system of records notice, http://www.ftc.gov/foia/sysnot/i-1.pdf, including disclosure to other government agencies. Submission of the requested information is voluntary, but failure to provide the requested information could delay processing or be a basis for rejection of your claim.

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

Yes. Use of OCS is voluntary. As noted earlier, individuals may submit their claims data by mail or facsimile if they do not wish to file their claim online through OCS. As explained in the Privacy Act statement, however, failure to submit the necessary claim data, whether online or by mailing of the completed form, may delay or result in rejection of the claim.

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

On the OCS website, individuals consent to their information being provided for all uses described in the FTC's Privacy Policy and the applicable FTC's Privacy Act statement. The claimant exercises these rights by choosing to complete, sign, and submit a claim form.

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

Claimants may request access to claims status and/or access to the claims data previously submitted by telephone, fax, or mail, to Rust, subject to verification of the claimant's identity, as necessary. The process for submitting requests for information pursuant to the Privacy Act of 1974, as to information that may be maintained by the FTC itself on the claim, if any, or data that Rust declines to make available upon request to a claimant, if any, is addressed in the Redress Program PIA.

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

The claims data that OCS collects and disseminates is sensitive, and unauthorized access or disclosure could result in identity theft or fraud. Those risks are controlled or mitigated in several ways.

First, access is limited by the login and authentication process described earlier. The security measure of requiring an individual to supply an email address before allowing access to the OCS website mitigates the risk of the information from a mailed notice being used to illegally access information on the website. If required, the email address could be tracked to determine the individual requesting access to the system.

Second, while logged into the OCS website, claimants will be able to enter or review/edit their information to ensure its accuracy prior to submitting their claim through the site for processing. Once the claim has been formally submitted through the site, the data are not maintained on the site, but are exported by secure means to data storage devices or facilities that are not accessible through the Internet, which mitigates the potential risk of unauthorized access or disclosure. *See* section 5.5 below. The stored claims data is then subject to other necessary and appropriate security controls to protect its confidentiality, integrity and availability, consistent with FISMA. Once the claim has been formally submitted to the site, claimants may request edits by contacting RUST via telephone, subject to verification of the claimant's identity, as necessary.

5. Web Site Privacy Issues

5.1 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.

Persistent tracking technology is not used by these websites, but temporary tracking technology is used to a limited extent to record the visit, pages requested, and unique users in order to evaluate the effectiveness and efficiency of the website as part of Rust's continuous improvement process. In addition, a temporary cookie is used for user session verification and is terminated at the end of the visit. This cookie does not hold any Personally Identifiable Information ("PII") nor can the information obtained be directly correlated to an individual claimant. Browsers should be closed to make sure cookies are properly expired after a claimant is finished with the website.

5.2 If a persistent tracking technology is used, ensure that the

proper issues are addressed (issues outlined in the FTC's PIA guide).

Not Applicable.

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

Rust websites are FIPS 140-2 compliant TLS v.1.0 (SSL 3.1) with 128-bit AES encryption with a 2048-bit RSA/SHA key 128-bit SSL encryption when personal information is collected through a web site, page, or online form.

Rust encrypts its backup data on tape or disk devices at 128-bit AES encryption or higher. For projects that have a business need for all data to be removed at the conclusion of services, Rust can accommodate this by segmenting this data out of normal backup rotations.

Rust utilizes a security layered approach to protecting the data entrusted to them in both transmission and at rest. They have deployed HIDS (host intrusion detection systems), NIDS (network intrusion detection systems), file integrity monitoring and an application firewall. Rust also utilizes services that monitor internal and external activities 365x24x7. This layered approach is consistent with FISMA standards.

5.4 Explain how the public will be notified of the Privacy Policy.

See Redress Program PIA and section 4.1 above.

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

The following privacy risk was identified for OCS websites: data provided by, or related to claimants, might be misused or improperly disclosed or accessed.

The risk identified above is mitigated by having all data exported at the conclusion of the claim form filing period to a secure data storage device that is not publicly accessible via the Internet.

In addition, Rust employs a significant number of layered technical controls to help prevent the misuse or improper disclosure of or access to consumer data. These controls include, but are not limited to:

- Hosting sites within a FISMA accredited boundary with all necessary and relevant controls in place (*see* Redress Program PIA).
- Administrative controls include a number of failed login attempts and a lockout.

5.6 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

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

The FTC follows all applicable FISMA requirements to ensure that information is appropriately secured at a moderate level.

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

Yes.

6.3 Has a risk assessment been conducted on the system?

Yes.

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

The technology employed to support FTC Redress Services does not raise any special privacy concerns not already addressed.

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

David M. Torok, Assistant Director
Division of Planning and Information
Bureau of Consumer Protection

Review:

Alexander C. Tang
Office of the General Counsel

Jeff Nakrin
Director, Records and Filings Office

Peter Miller
Acting Chief Privacy Officer

Margaret Mech
Chief Information Security Officer

Approved:

Jeff Huskey
Chief Information Officer