

**Federal Trade Commission
Privacy Impact Assessment**

for the:

ClaimTracker Website

January 2009

ClaimTracker Website Privacy Impact Assessment

Executive Summary

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, including Analytics, Inc., (Analytics) have been awarded a contract supporting RAO's goals. A comprehensive Privacy Impact Assessment (PIA) has been conducted for the BCP Redress Program and is available at <http://www.ftc.gov/os/2008/09/0809bcprepresspia.pdf> (Redress Program PIA).

Analytics proposes to use the ClaimTracker website (ClaimTracker) to provide individuals with the ability to review online the status of any claims that they have submitted. ClaimTracker is hosted on Analytics' FISMA (Federal Information Security Management Act) accredited network and employs processes and technologies covered in the Redress PIA. ClaimTracker resides on a separate domain than the Redress Database. A daily SQL Server Integration Services ("SSIS") automated procedure exports user claim number, HASH'ed password and claim status over a one-way trust between the Redress Database and ClaimTracker.

This Privacy Impact Assessment supplements the Redress PIA to address new issues raised by ClaimTracker. This PIA should be read in conjunction with the Redress PIA.

System Overview (Corresponds with Section 1 of the Redress Program PIA)

ClaimTracker provides claimants with an easily accessible point of contact to view the status of claims previously submitted to Analytics. As addressed in the Redress PIA, consumer information is collected first on claim forms which are returned to Analytics via the mail or facsimile. Claim forms cannot be submitted on ClaimTracker. Analytics will include a unique claim number, password and FTC Privacy Act Notice on each mailed claim form. Once the claim form is completed and returned to Analytics, the ClaimTracker website will update daily with the status of the individual's claim. The individual can obtain the status of their claim by accessing ClaimTracker with the password and claim number listed on their claim form. This authentication method limits claimants to their own information.

Analytics has used the ClaimTracker system in a number of other matters, including the Merrill Lynch Research Analyst settlement (which involved more than 1 million securities litigation claims regarding 23 separate securities), to provide a convenient, 24/7 secure method to frequently updated information to claimants regarding the status of their claims and general case information. This results in better informed claimants, and in our prior experience, a shortened time from notice to distribution.

ClaimTracker Website
Privacy Impact Assessment

Notice and Access for Individuals Information Collected and Stored within the System (Corresponds with Section 4 of the Redress Program PIA)

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

Users will be informed about what information is collected and how it is used by reviewing Analytics' Privacy Policy posted on the ClaimTracker website. This Privacy Policy clearly defines all information that is collected when visiting the site. ClaimTracker collects two categories of data: data entered into ClaimTracker by claimants seeking to review the status of a claim and web log information.

ClaimTracker will only collect two data elements from its users – the claim number and password – both of which are supplied by Analytics to consumers via a mailed claim form. ClaimTracker does not include or collect claimant name, address, or claim amount information.

In addition to the two data elements that users enter on ClaimTracker, ClaimTracker also collects standard web log information in an effort to prevent fraud, improve website quality, and assess the overall utility of the service, e.g. are claimants using the service? Information collected by ClaimTracker 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; pages requested, and the estimated time that a user spent on ClaimTracker. Analytics cannot correlate the data collected to identify specific users.

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

The FTC's Privacy Act Notice listed on the claim form explains the individuals' right to refuse to provide information and the associated consequences. The use of ClaimTracker is for the convenience of the consumer only and does not collect sensitive consumer information or impact an individuals' right or ability to receive redress or any substantive rights.

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

As explained in more detail in the Redress PIA, claimants 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 claimant exercises these rights by choosing to complete, sign and submit a claim form.

ClaimTracker Website
Privacy Impact Assessment

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

Claimants may request their information by telephone, fax, mail or email. The process for submitting requests for information pursuant to the Privacy Act of 1974 are addressed in the Redress PIA.

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

Consistent with the Redress PIA, the following privacy risk was identified: data provided by, or related to claimants, might be misused or improperly disclosed or accessed.

ClaimTracker does not collect, maintain, or disseminate sensitive Personally Identifiable Information (PII). ClaimTracker only includes for each claimant, a randomly assigned claim number and password, along with the status of any claim that they may have submitted. ClaimTracker does not collect, maintain, or disseminate name, address, or claim amount information.

Web Site Privacy Issues (Corresponds with Section 5 in the Redress Program PIA)

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 ClaimTracker website collects user IP addresses to identify attempted fraud. The number of visits, pages requested, and estimated time spent visiting the site are computed in order to evaluate the effectiveness and efficiency of ClaimTracker as part of Analytics' 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.

If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide). (5.2)

Not Applicable

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

Consistent with the Redress PIA, the ClaimTracker website uses 128-bit SSL encryption when this generic, non-personal information is collected.

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

ClaimTracker Website Privacy Impact Assessment

Analytics' Privacy Policy will appear on the ClaimTracker website.

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

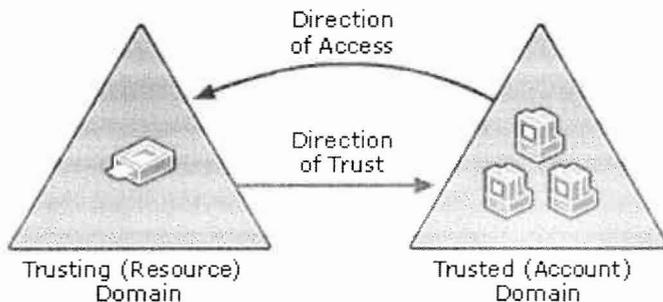
Consistent with the existing Redress PIA, the following privacy risk was identified: data provided by, or related to claimants, might be misused or improperly disclosed or accessed.

All data (randomly assigned password, claim number and claim status) is exported daily from the internal Analytics domain (which houses claimant information in the Redress Database) to the AISecure domain (which houses the ClaimTracker Database) through a one-way trust which is described below:

One-Way Trust

A one-way trust is a unidirectional authentication path created between two domains (trust flows in one direction, and access flows in the other). This means that in a one-way trust between a trusted domain (Analytics) and a trusting domain (AISECURE), computers in the trusted domain (Analytics) can access resources in the trusting domain. However, computers in the trusting domain (AISECURE), cannot access resources in the trusted domain.

Trust Path in a One-Way Trust



The data is pushed from the internal Analytics network redress database server to the AISecure database server using a SQL Server Integration Services (“SSIS”) package, **not a direct database-to-database link**. The package runs as a process separate from SQL Server, and is designed to simply copy selected data from the internal Analytics network redress server to the AISecure database server using an Object Linking and Embedding Database (“OLEDB”) data connection.

ClaimTracker Website Privacy Impact Assessment

The only plausible risk from this is the possibility of a buffer overflow in the OLEDB libraries used by SSIS from a maliciously crafted response from a compromised Demilitarized Zone (DMZ) server; however, OLEDB is a widely used and well vetted set of libraries, so this risk is negligible considering the security layers in place.

To mitigate this risk, Analytics employs a significant number of layered technical controls to help prevent the misuse or improper disclosure or access to consumer data. These controls include, but are not limited to:

- The ClaimTracker site is hosted by a FISMA accredited web server on the CARMEN network.
- ClaimTracker is maintained on a separate network than the redress database.
- Low risk PII is on the ClaimTracker site.
- Username and password authentication is negotiated via application layer security.
- Claimants are provided a unique claim number and a system generated alpha-numeric, case-sensitive password.
- Passwords are encrypted using a hash algorithm when transmitting between the web server and client based computing device.
- Administrative controls include three failed attempts and lockout, server event logging and IP address temporary tracking.

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). (5.6)

Not Applicable

Security of Information in the System (Corresponds with Section 6 in the Redress Program PIA)

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

Consistent with the existing Redress PIA, Analytics employs both information security and physical security to the privacy related information it collects. Analytics has received Federal Information Security Management Act ("FISMA", 44 U.S.C. § 3541, et seq.) and NIST certification as a moderate-security system.

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

Yes

Has a risk assessment been conducted on the system? (6.3)

ClaimTracker Website
Privacy Impact Assessment

Yes

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

Consistent with the existing Redress PIA, the technology employed to support FTC Redress Services does not raise any special privacy concerns not already addressed.

Prepared for the Business Owners of the System by:

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

Date: _____

Review:

Alexander C. Tang, Attorney
Office of the General Counsel

Date: _____

Marc Groman
Chief Privacy Officer

Date: _____

Margaret Mech
Chief Information Security Officer

Date: _____

Approved:

Stan Lowe
Chief Information Officer
Federal Trade Commission

Date: _____