

Federal Trade Commission  
Privacy Impact Assessment

**Analytics Class Action and Redress  
Management Enterprise Network  
(CARMEN)**

**Reviewed and Updated**

**May 2023**

## **Table of Contents**

1	System Overview .....	1
2	Data Type, Sources, and Use .....	2
3	Data Access and Sharing .....	4
4	Notice and Consent .....	6
5	Data Accuracy and Security.....	8
6	Data Retention and Disposal.....	10
7	Website Privacy Evaluation .....	10
8	Privacy Risks and Evaluation .....	10

# 1 System Overview

## 1.1 Describe the project/system and its purpose.

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) brings law enforcement actions that can result in the recovery of redress money from defendants for injured consumers or businesses. The FTC distributes money pursuant to a plan that is approved by a court, approved by an administrative law judge, or delegated to the FTC's discretion.

The Office of Claims and Refunds (OCR) is responsible for administering and coordinating refund activities, and Analytics Consulting LLC (Analytics) – an FTC notice and claim administration contractor – supports OCR's activities. This Privacy Impact Assessment (PIA) explains what Personally Identifiable Information (PII) OCR and Analytics collect throughout the refund administration process; who is allowed to use this information and for what purposes; and what steps are taken to identify and mitigate any privacy risks.

The Analytics Class Action and Redress Management Enterprise Network (CARMEN) system stores in a proprietary database consumer and business data provided by OCR or obtained directly from individuals who submit refund claims. In specific cases, Analytics might set-up an online claims submission website that permits individuals and businesses to submit an electronic claim.

Analytics uses the data from the system to fulfill its role as refund administrator,

ms im(r-6 tFo(c (raop-6 en(B))5 r((s))5  
Thss-16



refund matter. In routine refund matters, the data elements selected in table 2.1 are collected and maintained.

Additional non-PII data elements may include: business name (if needed), transaction data, transaction dates, product type, company selling product, customer number, customer account number, loss amount, and notes of claimant contact with Analytics, including any subsequent change requests, updates, corrections, etc. These notes may potentially contain PII. For example, a consumer may call Analytics to update their current address, phone number, etc.

In instances where a consumer calls Analytics regarding a refund matter, the Analytics Interactive Voice Response (IVR) system, which is hosted at the Genesys cloud and administered by Analytics, automatically logs the consumer's phone number and the date/time/length of the call for billing and routing purposes. If the consumer chooses to talk to a live agent, the call is routed to an Analytics contact center agent located in an Analytics facility. All consumers' calls to live agents are recorded. Details of calls may be summarized in the Analytics claims management system by claims processing staff.

### **2.3 What is the purpose for collection of the information listed above?**

Claimant information is collected, processed, stored, disseminated, or maintained by OCR staff and Analytics to identify potential claimants, to validate claimants and their claims, and to distribute refunds to appropriate claimants.

The Analytics CARMEN system maintains claimant information for verification and record-keeping purposes relating to refunds in FTC matters, as well as to calculate and distribute refund payments. These activities may include printing and mailing claim forms, processing claims and corrections submitted by claimants, issuing checks or other forms of payment, and providing consumer education.

Data collected by Analytics in a specific FTC matter may also be used by the FTC and Analytics to identify potentially fraudulent claims submitted in other FTC refund matters. For each refund matter managed by Analytics on behalf of the FTC, Analytics sends a complete list of claims filed to the FTC prior to the scheduled distribution. In an effort to identify potentially fraudulent claims, the FTC may analyze that information, refer back to data received in all refund matters past and present, and provide information regarding potentially fraudulent claims back to Analytics.

Claimant data collected by FTC and Analytics is also used to determine whether traditionally underserved groups are adequately being serviced when seeking redress. Redress recipient information is maintained in a restricted folder only accessible to authorized BE staff actively working on the analysis. When a new redress distribution is vetted and approved, files pertaining to that distribution are uploaded to the restricted folder. These files contain the following information pertaining to redress recipients: name, mailing address, loss amount, payment amount, and an assigned unique identifier. BE staff review the data in order to analyze and assess whether redress services are accessible and utilized by traditionally underserved

populations.

**2.4 What are the sources of the information in the system/project? How is the information collected?**

Source of Data

Data Will Be Accessed By and/or Provided To:	How and Why the Data Will Be Accessed/Shared
Analytics Staff	Authorized Analytics IT professionals have access to the





- Notice is provided via (check all that apply)
- Privacy Act Statement ( Written       Verbal)
  - FTC Website Privacy Policy
  - Privacy Notice (e.g., on Social Media platforms)
  - Login banner
  - Other
- (explain): \_\_\_\_\_

Notice is not provided (explain): \_\_\_\_\_

**D**

**4.2**



**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.**

Layers of technical and operational controls safeguard the data maintained within the CARMEN system

## 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?

Analytics and OCR will maintain the financial audit logs for claims and the records associated

with the records. The records will be retained for a period of 10 years from the date of creation. At the end of the retention period, the records will be securely destroyed. The records will be stored in a secure environment and will be protected from unauthorized access. The records will be backed up regularly and the backups will be stored in a secure environment. The records will be reviewed periodically to ensure that they are accurate and complete. The records will be used for the purpose of the project and will not be shared with any other party. The records will be maintained in accordance with the applicable laws and regulations. The records will be disposed of in a secure and confidential manner. The records will be destroyed using a secure method that ensures that the data is irretrievable. The records will be disposed of in a secure and confidential manner. The records will be destroyed using a secure method that ensures that the data is irretrievable. The records will be disposed of in a secure and confidential manner. The records will be destroyed using a secure method that ensures that the data is irretrievable.

Risk	Mitigation Strategy
or unnecessary sensitive PII data	before it is uploaded into CARMEN. To mitigate this, claim forms do not include open-text comment fields. Additionally, fields are configured to undergo data validation to ensure the requested information is entered. Claimants are also presented with the abilit4o-2 (t)sv(a)4 (l)-2 (i)-2 (da)4 (t)-2 t (l)-6 (ai)-6 (m)-6

**8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).**

Yes. The system is covered by [Privacy Act SORNs](#) for nonpublic FTC program records, FTC-I-1, and for computer system user and identification access records, FTC-VII-3. Consumers are assigned a unique ID that may be used to index and retrieve their system records for identification, tracking, and reporting purposes.

**8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?**

As described in sections 8.2 and 5.2, Analytics has technical and operational policies and controls in place to ensure data is safeguarded and to prevent misuse or accidental claims data modification. Analytics staff perform regular, ongoing reviews of system logs as part of their continuous monitoring process. The account management policies and controls in place to manage Analytics user accounts include the establishment, activation, modification, and termination of system accounts.

The collection, use, and disclosure of information from the Analytics CARMEN system has been reviewed to ensure consistency with the FTC's Privacy Policy.