Federal Trade Commission
Privacy Impact Assessment

Analytics Class Action and Redress Management Enterprise Network (CARMEN)

December 2019

Contents

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, including the following duties: (i) to intake and process claims filed; (ii) to answer questions from the FTC and other authorized parties; (iii) to answer questions from claimants and potential claimants; and (iv) to issue and track payments to authorized claimants.

Analytics maintains physical systems in their secure on-site location in Chanhassen, MN.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The FTC collects this information in order to provide refunds to injured consumers as part of its law enforcement activities pursuant to the FTC Act, 15 U.S.C. §§ 41-58, and other applicable statutes.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☐ User ID
☐ Date of Birth	☒ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Business name, unique claimant ID, customer account number, Analytics operators call summary, recorded calls with live agent.
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The claimant information that is collected, processed, stored, disseminated, or maintained within OCR or within the Analytics CARMEN proprietary database can vary, depending upon the 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

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

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.

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

Source of Data	***Type of Data Provided & How It Is Collected***
Individual Members of the Public	Initial source data comes from defendants' files and consumer complaints submitted to the FTC and transferred to Analytics; this includes the data elements listed in 2.1. Claimants also provide data directly to Analytics via phone or mail as part of the refund administration process.
Third Parties	Mailing address updates and corrections may be provided by third-party data sources such as the United States Postal Service (USPS), LexisNexis, Experian, CLEAR, etc.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
FTC Staff	FTC staff does not have direct access to the CARMEN system. Analytics shares claimant information and reports with the FTC via secure encrypted file transfer protocol or other secure file sharing technologies, all of which are encrypted with industry standard technologies both in-transit and at-rest.. The FTC reviews the data to ensure the redress distribution plan is implemented correctly and to ensure appropriate data security practices are in place.
Analytics Staff	Authorized Analytics IT professionals have access to the data for importing, validating, and storing claimant data. Authorized Analytics data analysts have additional access to perform mass updates, such as parsing names and USPS National Change of Address updates. Analytics claims processors assigned to work on a specific FTC matter are granted access to data for the purpose of validating eligibility, communicating with claimants, and updating claimants' contact information. Analytics management staff need to access the data for reporting, to supervise technology and processor resources, and to ensure accuracy and adherence to data handling standards. All Analytics employees with access to claimant information undergo background checks conducted by Analytics.
Claimants	If the claims and refunds matter requires that Analytics set-up a temporary website, individual claimants may submit information directly via online or hardcopy claim forms. Once claimants submit their information, they cannot, view or change their information online.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
Other External Parties	The FTC may share claimant information with law enforcement and other government agencies, courts, and defendants, or as otherwise authorized by law. OCR and Analytics securely download and transmit required data in response to authorized requests. Analytics may share data with third-party payment processors (banks, for example) in order to issue payments.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Analytics maintains formally defined roles and responsibilities, separation of duties, and access requirements for all employees.

All Analytics employees receive from Analytics Human Resources an initial (and annual refresher) privacy awareness or information security training, which includes a specific course related to PII. Additionally, all system users are required to read and acknowledge the Analytics Acceptable Use Agreement and relevant policies. Analytics Human Resources maintains electronic training records and logs.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

Analytics has developed an Incident Response Plan (IRP) to support the management, investigation, and response to incidents relating to PII. The plan contains a framework for responding to information security incidents, which include but are not limited to a violation of Analytics' computer security policies and standards, unauthorized computer access, loss of information confidentiality, and compromise of information integrity.

Every employee at Analytics has the responsibility to immediately report suspected or known breaches of the privacy or security of restricted information to the designated department or individual for their work area. This may be a system administrator, department management, or similar position. In the event of an incident, Analytics has a response team in place to respond quickly and rectify the situation. Contractual and legal requirements govern the timeframe for breach notification; Analytics must immediately report to the FTC any breach of FTC information.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

Claims and refunds cases that require Analytics to collect claimant information via a claim form will always provide claimants with a Privacy Act statement, whether the claim form is paper or Web-based. The Privacy Act statement explains the authority, purpose, and routine uses of the information to be collected; whether the information is voluntary or mandatory; and any consequences if the information is not collected (e.g., the FTC may be unable to pay the individual his or her refund claim).

Those claimants who submit consumer complaints to the FTC via the FTC online complaint form – as described in the Sentinel Network Services PIA – or via the FTC telephone complaint system (1-877-FTC-HELP), receive a similar Privacy Act statement at the time they submit their complaint. Their relevant consumer complaint information is then forwarded to Analytics for processing through the encrypted mechanisms outlined in section 3.1.

In some cases, the FTC may receive claimant information from a defendant's customer list, and a refund may be provided without the claimant having to take any action. In those instances, claimants are not provided with a Privacy Act statement; such claimants can learn about the FTC's collection, use, and disclosure of their information through the FTC's privacy policy, as noted below. In addition, all refund checks include a mailing address and/or telephone number for consumers to contact Analytics should they have any questions or concerns about their information.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☐ Other

(*explain*):_____

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

When the FTC obtains information from a defendant about injured consumers in order to mail them their checks, there is no opportunity for individuals to provide or decline to provide their information. Rather, this use of personal information is consistent with the purpose for which the FTC collects and maintains such consumer information from its defendants and allows the FTC to provide refunds efficiently and effectively to as many injured consumers as possible.

In cases where there is a claims process, individuals can decline to provide their information. If consumers choose to submit a claim, they are consenting to, and may not limit, the routine uses of their information stated in the applicable SORN (see Section 8.3) and Privacy Act statement. The consumer exercises this consent by choosing to complete, sign, and submit a claim form.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Claimants cannot access their records through the system online, but they may request access to their claims records by contacting Analytics via telephone or mail. Before making changes, Analytics asks consumers series of questions, including the tracking number and mailing address on file. The claimant is instructed to forward their change request in writing along with supporting documentation if needed. Analytics accepts written documentation via fax and mail. The system does not display/send PII as part of the inquiry process. If PII is collected and/or transmitted, encryption methods are implemented to protect sensitive information. Finally, claimants can obtain access to their own information through a Privacy Act request filed with the FTC's Freedom of Information Act (FOIA) Office.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Consistent with 4.3, claimants are provided with dedicated contact information to correct inaccurate or erroneous information. The process for receiving and responding to the requests is outlined in 4.3 and 5.1.

Claimants also can file a Privacy Act request through the FTC's FOIA Office to obtain access to their own information. The FTC FOIA Office will work with the claimant to respond to any complaints, concerns, or questions.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Various steps are taken to validate the accuracy and timeliness of collected data based on its original source. For example, prior to Analytics mailing a claim form, refund check, or consumer education material, claimant addresses are standardized and cross-checked against known data sources, such as the USPS National Change of Address Database and U.S. Postal Service records regarding street names and address ranges. All resulting additions, deletions, and changes to the data set are approved by the OCR and reconciled against the original source data.

In many instances, claimant data obtained from defendants' files can be used to mail refund checks directly to injured consumers and businesses. In other cases, individuals are contacted to provide or verify their information themselves. For example, claim forms may be mailed to a known set of claimants requesting that they validate, often under penalty of perjury, their address, loss amount, and entitlement to a refund. In other cases, claim forms will be made available to previously unknown claimants via case-specific notification and outreach. Again, claimants provide claim information, including their address, injury amount, and entitlement to a refund, often under penalty of perjury.

Analytics reviews claimant names, check distributions, and claim form responses to confirm that the loss amounts claimed are consistent with the established case-specific claim parameters.

OCR staff reviews data entry and decisions made by Analytics to ensure that the information remains accurate, complete, and up-to-date.

Outreach material, refund checks, and claim forms always include an FTC website address for additional information, a a telephone number and mailing address for consumers to contact the refund administrator to have their questions answered and/or to update their information.

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. Only authorized Analytics staff can access the system, on a need-to-know basis. The data is accessed via secure login. Analytics uses the data in accordance with the uses described in the company's contract with the FTC.

Prior to maintaining and disseminating claimant data, OCR staff removes all unnecessary information from the claimant data file. OCR staff only forwards encrypted data to refund administrators. Similarly, Analytics is instructed to collect the least amount of claimant information necessary.

If personal information is collected through an online form, it is protected by the Transport Layer Security (TLS) protocol using NIST-approved encryption algorithms.

Analytics has implemented a number of technical controls within the CARMEN system environment to help prevent misuse, or improper disclosure or access, to consumer data. These controls include, but are not limited to the following:

- Analytics websites are deployed on a separate network segment from the consumers' specific claims data;
- Username and password authentication is negotiated via application layer security;
- Claimants are provided a unique claim identifier and a system-generated password;

- Passwords are encrypted when transmitting between the web server and client based computing device;
- Administrative controls include a number of failed attempts and lockout, server event logging, and IP address temporary tracking.
- Data is encrypted in-transit and at-rest.

The Analytics CARMEN system uses a defense-in-depth strategy to protect system resources against attacks by utilizing security technologies and services that maintain the Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation requirements outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

Analytics' Development and User Acceptance Testing (UAT) environments utilize anonymized data.

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 issuing payments to claimants in accordance with NARA GRS 1.1, item 010, Financial Transaction Records, for six years. Any copies of matter-related documents received by Analytics and OCR, regardless of format, will be deleted or destroyed as non-records per the FTC NARA-approved records retention schedule, N1-122-09-1, Item 2.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Analytics does not host permanent websites on behalf of the FTC. However, Analytics may host a temporary website in a particular refund matter when the FTC determines it is appropriate and necessary to support online electronic claim submission. Persistent tracking technologies are not used on these temporary, matter-specific refund sites. Temporary session cookies are used for user session verification and are terminated at the end of the visit. These cookies do not hold any PII, and the information they contain cannot be directly correlated to an individual claimant. Analytics staff reviews each temporary website for compliance with the privacy requirements.

In compliance with the Privacy Act of 1974, the E-Government Act of 2002, guidance issued by OMB, and the FTC's own Privacy Policy, the FTC mandates that Analytics limit the collection of information from website visitors to the information necessary to assess and improve user experience, respond to consumer concerns, and administer claims and refunds.

To the extent that Analytics collects standard web log data, such as IP address, date and time of visit, and other required information, for cyber security and management reporting, such collection is in compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq.

8 Privacy Risks and Evaluation

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

Risk	***Mitigation Strategy***
Incomplete, inaccurate, redundant or unnecessary sensitive PII data	To reduce the risk of storing incomplete, inaccurate or unnecessary data and information, the Analytics data control team performs a verification and standardization process 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 ability to validate and verify their information before submitting. In order to minimize privacy risks, in the vast majority of redress matters, the information stored by Analytics is limited to name, contact information, and claim information, possibly coupled with validation under penalty of perjury. Comprehensive data security plans have been implemented to protect all data, including frequent, automated scans of information systems as well as policies and procedures to limit access to sensitive data and to ensure compliance with data privacy standards.
Misuse of data by individuals with access to PII or other sensitive information	Analytics employs Audit Trail logging to ensure all access to, or modification of data is logged. Audit data is stored in accordance with the Analytics data retention policy and in accordance with requirements set forth by the FTC. In all circumstances, audit data will be stored for no less than the lifetime of the engagement. Access to audit data is limited to those who have a reasonable business need and is not accessible by individuals who process claims and claimant information.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

The Analytics CARMEN system includes automated privacy controls to protect the privacy of victim data. Example controls include, but are not limited to:

- Role-based access based on business need;
- Assigned unique identifiers for all employees;
- Robust password requirements and policies;
- Multi-factor authentication for privileged accounts;
- Session termination after periods of inactivity;
- System lock-out after a certain number of failed attempts to log in;
- Automatic suspension of inactive accounts; and,
- Auditing and logging of system activities.

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.