Federal Trade Commission
Privacy Impact Assessment

Rust Consulting Claims Management Database Two (CMD2)

Reviewed February 2025

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 Rust Consulting, Inc. ("Rust")—an FTC notice and claim administration contractor—supports OCR's activities. This Privacy Impact Assessment (PIA) explains what Personally Identifiable Information (PII) OCR and Rust collect throughout the refund administration process, who is allowed to use this information and for what purposes, and what steps are taken to identify, secure, and mitigate any privacy risks to that information.

Rust's Claims Management System Database Two (CMD2) system stores in a proprietary database consumer and business data, provided by OCR or obtained directly from individuals who submit claims. In specific cases, Rust might set up an online claims submission (OCS) website that permits individuals and businesses to complete and submit an electronic claim.

Rust uses the data from the system to fulfill its role as the refund administrator, which includes 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 claimant; and (iv) to issue and track payments to authorized claimants.

Within the FTC, authorized Bureau of Economics (BE) staff have access to redress distribution data for analysis purposes.

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, Rust operators call summary, recorded live agent calls.
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☒ Social Security Number		
☐ Mother's Maiden Name		

The FTC does not routinely collect Social Security Numbers (SSNs) as part of its refund process. However, in limited cases, it may be necessary for the agency to collect and share SSNs with Rust in circumstances when the FTC must report the payments to the Internal Revenue Service (IRS) and provide 1099 Forms to the recipients. Form 1099 is a type of IRS form used to file and report various types of income other than wages and salaries.

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 Rust's CMD and OCS websites' proprietary databases varies depending upon the claims case. In routine claims matters, the data elements selected in Table 2.1 are collected and maintained.

[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.

Additional non-PII information 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 Rust, including any subsequent change requests, updates, corrections, etc. These notes may potentially contain PII. For example, a consumer may call Rust to update their current address, phone number, etc.

In instances where a consumer calls Rust regarding a claims matter, the Rust Interactive Voice Response (IVR), which is hosted at Rust facilities, 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 a Rust contact center agent located in Rust facility. All consumer calls to live agents are recorded. Details of calls may be summarized in the Rust 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 Rust to identify potential claimants, to validate claimants and their claims, and to distribute refund payments to appropriate claimants. In limited cases, the FTC may collect claimant SSNs and share the data with Rust. This is only done in cases where the FTC must report payments to the IRS and provide 1099 Forms to the claimants.

Rust's CMD2 system is used to maintain claimant information for verification and record-keeping purposes, and 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 Rust in a specific FTC matter may also be used by the FTC and Rust to identify potentially fraudulent claims submitted in other FTC claims and refunds matters. For each claim and refund matter managed by Rust on behalf of the FTC, Rust sends a complete list of claims filed to the FTC. In an effort to identify potentially fraudulent claims, the FTC may analyze that information, refer back to data received in all claims and refunds matters past and present, and provide information regarding potentially fraudulent claims back to Rust.

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	*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 Rust; this includes the data elements listed in 2.1. Claimants also provide data directly to Rust 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 CMD2 system. Rust 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. Authorized BE staff have access to redress distribution data in order to conduct analysis on the percentage of redress recipients belonging to traditionally underserved groups. 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 the redress recipients: name, mailing address, loss amount, payment amount, and an assigned unique identifier.
Rust Staff	Authorized Rust IT professionals have temporary access to the data for importing, validating, updating, and storing claimant data. Authorized Rust IT professionals have access to perform mass updates, such as parsing names and USPS National

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	Change of Address updates. Rust claims processors who are assigned to work on a specific FTC matter are granted access to data for the purpose of validating eligibility, communicating with claimants, and updating their contact information. Rust management staff need to access the data for reporting purposes, to supervise technology and processor resources, and to ensure accuracy and adherence to data handling standards. All Rust employees with access to claimant information receive background checks conducted by Rust.
Claimants	If the claims and refunds matter requires that Rust 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 orchange their information online.
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 Rust securely download and transmit required data in response to authorized requests. Rust may share with third-party payment processors (banks,for example) data necessary to issue payments to claimants.

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.

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

Rust employs formal, documented procedures to facilitate initial and annual refresher security and privacy awareness training, including a specific course related to PII, which is managed and implemented by Rust's Security Team and Human Resources. Additionally, all system users are required to read and acknowledge all relevant policies.

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.

Rust has a documented Security Management and Incident Response Procedure which includes appropriate responses when an incident is detected, a communications plan, and a plan for IR testing. This procedure is updated annually, or as business requires. Security incidents detected are promptly contained, investigated, resolved, and reported to management. Rust management and security team are responsible for notifying FTC officials of any event or incident impacting the security or integrity of FTC data.

Incident response is included in the required annual Security Awareness Training taken by all employees.

Breach notification timeframe is governed by contractual and legal requirements; Rust must immediately report to the FTC all breaches of FTC materials and 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 Rust 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 Rust 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 Rust should they have any questions or concerns about their information.

☒ 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): _____

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 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 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 to their claim record by contacting Rust by phone or mail. Before making changes, Rust asks callers a series of questions, including the reference number assigned by Rust and mailing address on file. If the claimant identity is confirmed, a change of address can be made over the phone. For other changes, the claimant is required to forward their change request in writing along with supporting documentation. Rust accepts written documentation via fax, mail, or email. 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.

As stated above in Section 4.3, claimants can request corrections to any inaccurate information by contacting Rust, validating their identity, and forwarding the change request in writing along with any supporting documentation as necessary.

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 Rust 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 data.

In many instances, claimant data obtained from defendants' files can be used to mail refunds 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 refunds. 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 refund, often under penalty of perjury.

Rust 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 Rust 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, as well as 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 Rust's CMD2 system. Only authorized Rust staff can access the system, on a need-to-know basis. Data usage is in accordance with the uses described in the executed contract between the FTC and Rust to support the FTC's claims and refunds activities. Prior to maintaining and disseminating claimant data, OCR staff removes all unnecessary information from the claimant data file and encrypts all data transmitted to Rust via email. Rust encrypts claimant data at rest. In addition, the FTC instructs Rust to collect the least amount of claimant information necessary. If personal information is collected through an online form, appropriate Transport Layer Security (TLS) encryption algorithm is used to protect the information. Rust 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 Standardsand Technology (NIST) Special Publication 800-53.

There are several additional safeguards in place to protect the data and to prevent the misuse or improper disclosure or access to consumer data. These controls include, but are not limited to the following:

- OCS websites are maintained on a separate network segment from the consumers' specific claims data;
- Claimants are provided a unique claim identifier which is used for identify when they contact Rust;
- Technical controls include accounts lock out after a number of failed login attempts, and application is only internally accessible through an encrypted web-browser using TLS;
- All data stored and transmitted within Rust's secure, layered environment is encrypted to mitigate risks;
- Full encrypted backups of all production data are routinely conducted, and they are store at a separate and secure location;
- Audit trails maintain a record of authorized and unauthorized system events both by system and application processes and by user activity of systems and applications. Audit logging is continuous, and logs are archived to provide access for review.

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?

Development and User Acceptance Testing (UAT) environments are physically and logically separate from that of production, and UAT mirrors production as closely as possible at both the hardware and software levels. FTC data is not used in UAT environments. Any exception would require prior FTC approval, and data would be deleted immediately upon remediation.

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?

Disposition of general technology management records and information system security records is authorized under National Archives and Administration (NARA) General Records Schedules 3.1 and 3.2. The disposition of the data will be covered by NARA-approved records disposition schedules of the FTC.

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.

Rust does not host any permanent websites on behalf of the FTC. However, Rust may host a temporary website in a particular claims and refunds matter when the FTC determines it is appropriate and necessary to support online electronic claim submission. Persistent tracking technologies will not be used on these temporary, matter-specific claims and refunds 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 obtain cannot be directly correlated to an individual claimant. Rust 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 Rust 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 Rust's web hosting provider 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 Modernization 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, Rust's data control team performs a verification and standardization process before it is uploaded into CMD2. 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 Rust 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	Rust employs Audit Trail logging to ensure all access to, or modification of, data is logged. Audit data is stored in accordance with Rust's 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 Rust CMD2 application has built-in privacy controls, including role-based access controls, masking full or partial data fields containing PII which is not relevant to the specific tasks assigned to the employee, and implementing the technical and operational controls described in section 5.2.

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 5.2 and 8.2, Rust has technical and operational policies and controls in place to ensure data is maintained safeguarded and to prevent misuse or accidental claims data modification. Third party auditors have assessed Rust information security controls and evaluated their effectiveness. Rust has established monitoring controls to ensure systems are secure and operating effectively.

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