Federal Trade Commission
Privacy Impact Assessment

Simpluris Cadence Platform (Simpluris)

Published

April 2024

Table of 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. Within BCP, the Office of Claims and Refunds (OCR) is responsible for administering and coordinating refund activities and has procured the services of Simpluris Cadence Platform (Simpluris) to support redress and claims functions. Simpluris is responsible for maintaining personally identifiable information and FTC non-public information securely and confidentially. OCR provides Simpluris with data and information concerning the reporting and distribution proceeds from FTC claims and settlements. Although OCR provides the PII, Simpluris, as the administrator, reviews and assists with the distribution plan. This includes developing a timeline for distribution; locating and identifying eligible consumers; conducting the notice and claims process; and processing and distributing payments.

The FTC shares data with Simpluris that includes claimant data from the defendant/respondent's records, records obtained during the FTC's investigation, along with consumer complaint information from the Sentinel Network Services (SNS)[1]. Simpluris may collect personal information directly from potential claimants via website, third-party data, email, fax, text message, physical mail, phone, or any other method deemed necessary in relation to the contracted duties as required by the FTC. Any information received is only used for the express purpose of administering the case or project, such as verification of case involvement, claim validation, tax reporting and verification, and redress calculations and payments. Additionally, Simpluris may be asked or required by the FTC to gather information from third-party sources to fulfill their administration duties, comply with FTC orders and plans, or comply with the direction of the tax administrator.

Simpluris is committed to protecting the FTC security of non-public personally identifiable information. FTC security policies and processes have been developed and implemented for storing, using, and disposing of such information provided during their administration duties. Access is strictly enforced based on the concept of least privilege.

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.

[1] For more information, refer to the SNS Privacy Impact Assessment available online.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[2] 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		
☒ 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, Simpluris 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		

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.

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 Simpluris, including any subsequent change requests, updates, corrections, etc. These notes may potentially contain PII. For example, a consumer may call Simpluris to update their current address, phone number, etc. Simpluris also anticipates using evidentiary info for FTC claims (e.g., proof of purchase, educational records, vehicle records, etc.) to support case specific projects.

[2] 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.

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 Simpluris to identify potential claimants, to validate claimants and their claims, and to distribute refunds to appropriate claimants.

The Simpluris Cadence system maintains claimant information for verification and recordkeeping 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 Simpluris in a specific FTC matter may also be used by the FTC and Simpluris to identify potentially fraudulent claims submitted in other FTC refund matters. For each refund matter managed by Simpluris on behalf of the FTC, Simpluris 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 Simpluris.

Claimant data collected by FTC and Simpluris 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 population.

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 Simpluris; this includes the data elements listed in 2.1. Claimants also provide data directly to Simpluris 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 do not have direct access to the Simpluris Cadence system. Simpluris shares claimant information and reports with the FTC via secure encrypted file transfer protocol (SFTP) 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.
Simpluris Staff	Data is provided, accessed, and shared by authorized Simpluris employees based on limited role-based permissions access hierarchy for individuals handling the FTC project. Sharing and transfer of data between the FTC and Simpluris is encrypted using the FTC's SFTP, or other secure methods approved by the FTC. Authorized Simpluris IT professionals have access to the data for importing, validating, and storing claimant data. Authorized Simpluris data analysts have additional access to perform mass updates, such as parsing names and USPS National Change of Address updates. Simpluris 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. Simpluris 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.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	All Simpluris employees with access to claimant information undergo background checks conducted by Simpluris Human Resources.
Claimants	If the claims and refunds matter require that Simpluris 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.
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 Simpluris securely download and transmit required data in response to authorized requests. Simpluris may share data with third-party payment processors (banks, for example) in order 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.

Simpluris maintains formally defined roles and responsibilities, separation of duties, and access requirements for all employees. All Simpluris employees receive initial (and annual refresher) privacy awareness and role-based information security training. Access to the Simpluris Cadence system is only granted after the user has taken the training with the Acceptable Use Policy that provides guidance on protecting sensitive information. The security awareness training program is administered under the oversight of the Simpluris Director of Information Technology.

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.

Simpluris has defined its incident handling capability within the Incident Response Plan and Procedures document for security incidents. The plan includes preparation, detection and analysis, containment, eradication, and recovery. The incident response capability is incorporated in the contingency planning activities. Simpluris conducts incident management training, awareness, and testing scenario-based sessions annually with quarterly communications distributed company-wide covering details concerning incident response responsibilities, enforcing processes, and policies.

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 Simpluris to collect claimant information via a claim form provides claimants with a Privacy Act statement, whether the claim form is paper or electronic. 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 Simpluris 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 Simpluris 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 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 Simpluris via telephone or mail. Before making changes, Simpluris asks consumers series of questions to verify their identity, 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. Simpluris 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 Simpluris 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.

Simpluris 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 Simpluris 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 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.

Third party audits and risk assessments are performed annually. Least privileged access is employed to ensure that Simpluris employees only have access to what is required to perform their job duties. Access controls ensure that only authorized users with network credentials can access the Cadence system. Encryption is provided for data in transit and at rest. Access to the backend data in Amazon Web Services (AWS) is also controlled through strict access controls, including Multi Factor Authentication (MFA), and limited to only authorized personnel. The Director of Technology and Program Management Office at Simpluris is responsible for ensuring proper user of data.

Additionally, Privacy and Security Awareness training is provided to employees on an annual basis using the KnowBe4 platform. This training provides Simpluris employees with proper data handling techniques and emphasizes the need to safeguard protected data. Also, per its contract with the FTC, all Simpluris staff working on FTC Redress matters receive training regarding FTC standards, guidelines, and regulations required for data privacy/security and recordkeeping.

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?

☒Not Applicable. Simpluris does not use PII in the system testing, training, or research.

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?

Simpluris 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 Simpluris and OCR, regardless of format, will be deleted or destroyed as non-records per NARA-approved records retention schedules.

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.

Simpluris does not host permanent websites on behalf of the FTC. However, Simpluris 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. Simpluris 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 Simpluris 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 Simpluris 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 (FISMA), 44 U.S.C. § 3551, 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,	To reduce the risk of storing incomplete, inaccurate, or unnecessary data and information, the Simpluris data control team performs a verification and standardization process

Risk	*Mitigation Strategy*
or unnecessary sensitive PII data	before it is uploaded into Cadence. 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 Simpluris 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	Simpluris employs a Security Event Information Management system (SEIM) to ensure all access to, or modification of data is logged. Audit data is stored in accordance with the Simpluris 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 one year. 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.

Simpluris uses both automated and enhanced capabilities to ensure privacy is maintained. Combining the principles for least privileged access, role-based security, data loss prevention, labels, and alerting with logging. Simpluris policies and systems require automatic lockout of inactive systems and devices after a specified period of time, as well as after a specified number of failed login attempts. Simpluris utilizes MFA and Single Sign On (SSO) features to protect systems and applications from unauthorized access. Centralized monitoring and logging tools, including a SEIM solution, aggregate security events and raise alerts to staff based on risk.

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, Simpluris has technical and operational policies and controls in place to ensure data is safeguarded and to prevent misuse or accidental claims data modification. Simpluris 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 Simpluris user accounts include the establishment, activation, modification, and termination of system accounts. The collection, use, and disclosure of information from the Simpluris Cadence system has been reviewed to ensure consistency with the FTC's Privacy Policy.