Date of Approval: 04/23/2026
Questionnaire Number: 2932

# Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

FTC Delivery of Identity Theft Data to IRS, 14039-SDT

Business Unit

Taxpayer Services

Preparer

# For Official Use Only

Subject Matter Expert

# For Official Use Only

Program Manager

# For Official Use Only

Designated Executive Representative

# For Official Use Only

Executive Sponsor

# For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

The Federal Trade Commission (FTC) delivery of identity theft data to the Internal Revenue Service (IRS), referred to as 14039-SDT, is a process that allows individuals to report tax-related identity theft in a simple and efficient way. When a person reports identity theft through FTC's IdentityTheft.gov website, they can choose to have their information sent directly to the IRS to complete Form 14039, Identity Theft Affidavit. This removes the need for the individual to separately contact the IRS and submit the same information again. The IRS Office of Identity Protection Strategy and Oversight (IPSO), within Taxpayer Services, owns and operates this process. IPSO employees receive and review the information submitted by individuals, categorize the cases, and ensure they are processed appropriately to protect taxpayer accounts. This process supports Section 2 of Executive Order 13681, Improving the Security of Consumer Financial Transactions, which directs federal agencies to reduce the burden on individuals affected by identity theft and improve the time it takes to resolve these cases. The primary users of this process are IRS employees within Identity

Protection Strategy and Oversight who are responsible for reviewing and managing identity theft cases. This process benefits the IRS by improving service to taxpayers and increasing efficiency. It allows individuals to report identity theft in one place and ensures the IRS receives timely and accurate information to take action. By simplifying reporting and speeding up case handling, the IRS can better protect taxpayers and uphold its mission to provide quality service and safeguard taxpayer information.

# Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

The FTC collects PII from individuals through IdentityTheft.gov to complete IRS Form 14039. Individuals are provided with required privacy notices and may retain a copy of their submission. Each submission is assigned a unique FTC identifier and transmitted to the IRS via encrypted batch files using Secure Large File Transfer (SLFT) in accordance with federal security standards. IRS Identity Protection systems extract the data into a secure SQL Server environment. Each record is assigned an IRS ID while retaining the FTC ID to ensure traceability. Data is converted into Form 14039 PDF and processed using standard procedures. Processing events (e.g., receipt, extraction, conversion, duplicate status, review status) are logged. Failed transmissions are identified, reported, and reprocessed. Access is restricted through role-based controls to authorized personnel. User actions are logged with SEID and timestamps. Data is categorized and securely transmitted to the Fresno campus for ingestion into Correspondence Imaging Inventory (CII). Information is used solely for identity theft resolution and protected under IRC Â§6103. Data is maintained in IRS systems of records (Treasury/IRS 00.001) with access controls enforced. Only data necessary for case processing is retained. Records, including PDFs and logs, are maintained per NARA-approved schedules and IRS policies. Individuals may contact Identity Theft Victims Assistance (IDTVA) to access or correct their information. After authentication, Customer Service Representatives (CSR) may disclose information, document updates, and make corrections as appropriate. The FTC purges SSNs and CAF data after successful transfer. IRS records are destroyed per NARA schedules using approved sanitization methods, including backups. Safeguards include encryption, audit logging, monitoring, and incident response in accordance with FISMA, OMB, and NIST standards.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address
Family Members
Federal Tax Information (FTI)
Individual Taxpayer Identification Number (ITIN)
Name
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Telephone Numbers
Universal Unique Identifier (UUID)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for tax returns and return information - IRC section 6109

# Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

Project

3 What Tier designation has been applied to your system? (Number)

0

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

7763

4.12 What is the previous PCLIA title (system name)?

FTC delivery of identity theft data to IRS, 14039-SDT

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

Expiring PCLIA

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

TS-CAS-AM-Identity Protection Strategy & Oversight staff in partnership with another Federal Agency, The Federal Trade Commission.

9 Is this System listed on As-Built-Architecture (ABA)? If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

No

10 Does this system disclose any PII to any third party outside the IRS?

No

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Individuals who submit identity theft information through the FTC IdentityTheft.gov website are provided opportunities to access and correct their information both prior to and after it is received and maintained within IRS systems. At the time of submission, individuals may print or otherwise retain a copy of their FTC report and the generated IRS Form 14039. Certain sensitive

data elements, such as the Social Security Number and CAF number, are redacted. Form 14039 includes information regarding the individual's rights and applicable procedures. After the information is received by the IRS, individuals may contact the Identity Theft Victim Assistance (IDTVA) function to request access to their information or inquire about the status of their case. Upon successful authentication, IRS Customer Service Representatives (CSRs) are authorized to disclose relevant account information, confirm receipt and processing status, and explain how the information is being used. If an individual identifies inaccuracies or wishes to provide additional information, the individual may do so through the CSR. The CSR will document the information, make updates to IRS systems as appropriate, and, when necessary, refer the case for further review. Supporting documentation may be required to validate requested changes. Individuals may also submit corrections or additional information in writing by responding to IRS correspondence or by mailing documentation to the appropriate IRS function, in accordance with instructions provided in IRS notices or publications. In addition, individuals may seek assistance through the Taxpayer Advocate Service (TAS), which provides an independent mechanism to address unresolved issues or concerns regarding the handling of their information. These processes operate in addition to the access and amendment rights available under the Privacy Act and the Freedom of Information Act (FOIA) and provide multiple administrative avenues for individuals to review and request correction of their information.

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

IRS employees have the following access level, Users: Read Write, Managers: Read Only, System Administrator: Administrator, Developers: Read Write

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

The IRS does not collect the information from the victim. FTC's identitytheft.gov collects the information and utilizes 'opt-in' process to confirm a victim (individual) voluntarily wants to provide specific complaint data that's collected in fields of an IRS Form 14039. The 'opt in' and 'opt out' functionality is housed on the FTC website, identitytheft.gov, and records the individual's choice to forward the Form 14039 to the IRS or not. The full privacy notice is listed on the Form 14039 and is listed below in this response. Our legal authority to request the information is 26 U.S.C. 6001. The primary purpose of the form is to provide a method of reporting identity theft issues to the IRS so that the IRS may document

situations where individuals are or may be victims of identity theft. Additional purposes include the use in the determination of proper tax liability and to relieve taxpayer burden. The information may be disclosed only as provided by 26 U.S.C. 6103. Providing the information on this form is voluntary. However, if you do not provide the information it may be more difficult to assist you in resolving your identity theft issue. If you are a potential victim of identity theft and do not provide the required substantiation information, we may not be able to place a marker on your account to assist with future protection. If you are a victim of identity theft and do not provide the required information, it may be difficult for IRS to determine your correct tax liability. If you intentionally provide false information, you may be subject to criminal penalties. You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by section 6103. Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can write to the Internal Revenue Service, Tax Products Coordinating Committee, SE:W:CAR:MP:T:T:SP, 1111 Constitution Ave. NW, IR-6526, Washington, DC 20224. Do not send this form to this address. Instead, see the form for filing instructions. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Not Applicable

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

100,000 to 1,000,000

22 How is access to SBU/PII determined and by whom?

The data provided by FTC is transmitted to IRS using Governmental Liaison (GL)'s Secure Data Transfer (SDT) and it resides on a secure IRS server. Access

to the server is administered via Business Entitlement Access Request System (BEARS) requests and is granted by the IRS Identity Protection Strategy and Oversight (IPSO) office Subject Matter Expert (SME) on a 'need-to-access' basis. An IPSO based SME will oversee server access. There are only four IRS employees with access to the server at any time, one primary point of contact (POC) in IPSO and their backup.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

The primary privacy risk in this process is the potential unauthorized disclosure of sensitive taxpayer information during transmission from the Federal Trade Commission (FTC) to the Internal Revenue Service (IRS), as well as during receipt, processing, and internal transfer by Identity Protection Strategy and Oversight (IPSO). Because the information becomes return information under Internal Revenue Code (IRC) §6103 upon receipt by the IRS, any improper access or disclosure could adversely impact taxpayer privacy and civil liberties. To mitigate these risks, data transmitted from the FTC is encrypted and transferred using secure methods. Upon receipt, IPSO personnel access the data within a controlled environment using role-based access controls, ensuring only authorized users with a need to know can view or process the information. User actions, including access and processing activities, are logged with user identifiers to support accountability. During processing, IPSO assigns identifiers, categorizes cases, and prepares records for further handling. When data is transferred internally to the Correspondence Imaging Inventory (CII) system, the transfer is conducted through secure IRS processes designed to prevent unauthorized access or interception. In accordance with IRC §6103(p)(3)(A), the IRS maintains records to account for disclosures of return information, including internal disclosures, documenting what information was shared, with whom, and for what purpose. These records support oversight and ensure compliance with statutory requirements. Where applicable, disclosures are also managed in accordance with subsection (c) of the Privacy Act. These controls help ensure that sensitive data is protected throughout transmission, processing, and internal transfer, and that all disclosures are properly documented and auditable.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

Each file sent by the FTC is given a unique ID by the FTC. When the IRS receives the file, Identity Protection (IP) staff load the data into a secure SQL Server database and assign their own record ID, while keeping the FTC’s original ID for tracking. The system keeps a detailed log for each file. This log includes:

The date the FTC created the file and sent it, confirmation that the file was successfully received and processed, whether the data was converted into a PDF Form 14039, and the date of that conversion, whether the submission is a duplicate, the current status of the file (for example, under review or review completed), the employee ID (SEID) of the person who reviewed the file, and the category code assigned to the case. Designated staff review each submission to make sure it is placed in the correct category for processing. After the data is extracted, IP sends a confirmation email to the FTC on the next business day. This email confirms the total files received and total successfully processed. Once cases are categorized, IP generates the necessary forms and sends them to a campus support team in Fresno. That team uploads the files into the Correspondence Imaging Inventory (CII) system for employee case assignment. Records associated with FTC-submitted Form 14039 data are maintained in accordance with Internal Revenue Manual (IRM) 1.15, Records and Information Management, and the IRS Records Control Schedules (RCS) contained in Document 12990, approved by the National Archives and Records Administration (NARA). These records fall under Accounts Management taxpayer correspondence and case files (Treasury/IRS 00.001) and are retained for 7 years after case closure, after which they are destroyed in accordance with approved disposition requirements. Data maintained in temporary processing systems is retained only as long as necessary to support processing and is not considered the official record.

27 Does this system use or plan to use SBU data in a non-production environment?
No

# Interfaces

**Interface Type**
IRS Systems, file, or database
Agency Name
Correspondence Imaging Inventory (CII)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secure email/Zixmail

**Interface Type**
IRS Systems, file, or database
Agency Name
EFTU-GUF
Incoming/Outgoing
Both

Transfer Method
Electronic File Transfer Utility (EFTU)
Other Transfer Method
Executable Application

**Interface Type**
Other Federal Agencies
Agency Name
FTC
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Kiteworks

**Interface Type**
IRS Systems, file, or database
Agency Name
IRS Remote Server
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Kiteworks

# Systems of Records Notices (SORNs)

**SORN Number & Name**
IRS 00.001 - Correspondence Files and Correspondence Control Files
Describe the IRS use and relevance of this SORN.
To track correspondence (Form 14039, Identity Theft Affidavit).

**SORN Number & Name**
IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
The FTC will transmit completed Forms 14039 (Identity Theft Affidavit) for victims that opt-in to have FTC share it with the IRS. The IRS will process Form 14039 as they do all other Forms 14039. The benefit to victims is reduced burden in reporting and decreased recovery time. This also helps improve victim assistance response time on behalf of the IRS.

**SORN Number & Name**
IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

This system supports oversight of data received from the Federal Trade Commission (FTC) by recording user access and system activity within Identity Protection Strategy and Oversight (IPSO). Audit records include user identifiers (SEID), dates and times of access, and actions taken during intake, processing, and transfer to the Correspondence Imaging Inventory (CII). These records are used to monitor system use, identify and investigate potential unauthorized access to taxpayer information, and support compliance with Internal Revenue Code (IRC) 6103 by ensuring accountability for access to sensitive data.

**SORN Number & Name**

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

The FTC will transmit completed Forms 14039 (Identity Theft Affidavit) for victims that opt-in to have FTC share it with the IRS. The IRS will process Form 14039 as they do all other Forms 14039. The benefit to victims is reduced burden in reporting and decreased recovery time. This also accomplishes improved victim assistance response time on behalf of the IRS.

**SORN Number & Name**

IRS 42.021 - Compliance Programs and Projects Files

Describe the IRS use and relevance of this SORN.

Form 14039 may be used to report identity theft occurring from a fraudulent tax return submission. The fraudulent returns may be tax evasion schemes or noncompliance schemes.

# Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

TAX ADMINISTRATION - TAXPAYER SERVICES DIVISION (FORMERLY WAGE AND INVESTMENT, W&I) RECORDS

What is the GRS/RCS Item Number?

29 Item 56(4)(c), Item 439(a)(b), Item 446

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Item 56-Income Tax Returns Filed by Individuals, Partnerships and Fiduciaries/(c) Filed with returns in potential refund litigation

case files. Returns and all related documents. Item 439 (A) or (B)-Fraudulent Tax Scheme Files. Item 446-IRS Identity Validation (Out of Wallet) System.

What is the disposition schedule?

Item 56(4)(c) Cut off at end of CY in which case is closed. Retire (paper records) to Records Center 3 years after cutoff. Destroy 10 years after cutoff. Item 439(a) Delete/Destroy when no less than 5 years old, but not to exceed 10 years old. Item 439(b) Not Applicable. See RCS 30, Item 40 for disposition. This series is scheduled under Job No N1-58-07-11, Items 1(a) through 1(d). Item 446(c) Cut off at the end of the calendar year (in which data is received from FS). Delete data 7 years after cutoff.

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

TAX ADMINISTRATION - COLLECTION

What is the GRS/RCS Item Number?

28 Item 6(a)

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Item 6(a)-National Fraud Program Case Files. These records include copies of documents related to fraud cases such as Form 11661, Form 11661A, Form 2797, written plans of action, emails, notes from the Fraud Technical Advisor and miscellaneous other documents.

What is the disposition schedule?

Cut off when case is closed. Destroy 3 years after the case is closed.

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

IRS TAX PRACTITIONER ENROLLMENT, PROFESSIONAL RESPONSIBILITY, AND AGENT PRACTICES

What is the GRS/RCS Item Number?

11 Item 15

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Complaint Case Files. Files consist of Forms 14157, 3949-A, complaint letters, internal, email complaints and/or documents that support the complaint. Other forms such as Form 14157A (Return Preparer Fraud or Misconduct Affidavit), Form 843 (Claim for

Refund or Request for Abatement), and Form 14039 (Identity Theft Affidavit) may also be included. Additional information may include case closing check sheets, penalty calculation check sheets, correspondence sent to solicit more information from the complainant, correspondence sent to warn and educate the return preparer, case research documents or printouts from databases such as IDRS, Accurint, and EUP. (RPO Job No. DAA-0058-2013-0015-0001)

What is the disposition schedule?

Cut off at end of processing year in which case is closed. Transfer to off-site storage when no longer necessary. Destroy 7 years after cutoff.

# Data Locations

What type of site is this?

System

What is the name of the System?

Correspondence Imaging Inventory (CII)

What is the sensitivity of the System?

Federal Tax Information (FTI)

Please provide a brief description of the System.

The Correspondence Imaging Inventory (CII) is an inventory system for scanning Accounts Management receipts into digital images and working the cases from those images.

What are the incoming connections to this System?

Secure e-mail. Identity Protection Strategy and Oversight convert FTC data files into processible Form 14039s. These are sent by secure email to campus support teams in Fresno to be injected into the CII pipeline.

What are the outgoing connections from this System?

Data remains within IRS systems and is not transmitted outside the IRS as part of this workflow.

What type of site is this?

System

What is the name of the System?

SQL Server

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

Secure IRS Database Server

What are the incoming connections to this System?

Secure Data Transfer

What are the outgoing connections from this System?

Correspondence Imaging Inventory