MANUAL TRANSMITTAL

25.23.1

Department of the Treasury
Internal Revenue Service

SEPTEMBER 21, 2022

EFFECTIVE DATE

(10-01-2022)

PURPOSE

(1) This transmits revised IRM 25.23.1, Identity Protection and Victim Assistance - Policy Guidance.

MATERIAL CHANGES

(1) IRM 25.23.1.2(6) Removed reference to ITAR program and updated to include IDTX program.

(2) Exhibit 25.23.1-1 Removed requirement to complete form 14103.

(3) Various editorial changes made throughout and updated links.

EFFECT ON OTHER DOCUMENTS

IRM 25.23.1 dated September 07, 2021 is superseding and includes no IRM procedural updates.

AUDIENCE

The provisions in this manual apply to all divisions, functional units, employees, and contractors within the IRS working identity theft cases.

Karen A. Michaels
Director, Accounts Management
Wage and Investment Division

25.23.1
Identity Protection and Victim Assistance - Policy Guidance

Table of Contents

25.23.1.1 Program Scope and Objectives
25.23.1.1.1 Background of the Identity Protection Program
25.23.1.1.2 Terms/Definitions/Acronyms
25.23.1.1.3 Related Internal Revenue Manuals (IRM) and other Reference Materials
25.23.1.2 Wage and Investment - Accounts Management - Identity Protection Strategy and Oversight (IPSO)
25.23.1.2.1 Identity Protection (IP) Program Responsibilities
25.23.1.2.2 Identity Theft Victim Assistance (ITVA)- Program Responsibilities
25.23.1.3 Identity Theft and the IRS
25.23.1.3.1 Identity Theft in Tax Administration
25.23.1.4 IRS Employees Who May be Victims of Tax-Related Identity Theft
25.23.1.4.1 IRS Employees Who May be Victims of Non-Tax-Related Identity Theft
25.23.1.5 Identity Protection and Victim Assistance Initiatives
25.23.1.5.1 Awareness Training and Education
25.23.1.5.2 Guidance to Implement Section 1402 of the Taxpayer First Act
25.23.1.6 Data Breach - Business Entities Whose Employees or Clients PII was Breached
25.23.1.7 Taxpayers who are Victims of a Data Breach

Exhibits
25.23.1-1 Glossary of Identity Protection Terms and Definitions
25.23.1-2 References

25.23.1.1
(09-19-2017)
Program Scope and Objectives

(1) **Purpose:** This manual defines the mission, objectives, and governance structure of the Identity Protection and Victim Assistance Program. It provides the organizational framework for carrying out specific policies and procedures aimed at preventing identity theft (IDT), protecting taxpayers and helping victims of identity theft.

(2) **Audience:** The primary users of the IRM are anyone working identity theft inventory and helping victims of identity theft.

(3) **Policy Owner:** The Director of Accounts Management.

(4) **Program Owner** Accounts Management - Identity Protection Strategy and Oversight (IPSO).

(5) **Primary Stakeholders** Taxpayers who are victims of identity theft and the employees working to assist them.

(6) **Program Goals:**

- The development of short-term and long-term remedies to protect taxpayer information and make the experience of those who are already victims faster and more efficient.
- The development of Servicewide policy, procedures, and guidelines for the priority of recognizing, marking and acknowledging individual taxpayer claims involving identity theft.
- Support of IPSO activities within the scope of programs associated with identity protection.

25.23.1.1.1
(03-04-2020)
Background of the Identity Protection Program

(1) Identity theft places a burden on its victims and presents a challenge to businesses, organizations and government agencies, including the Internal Revenue Service (IRS).

(2) The IRS combats tax-related identity theft with an aggressive strategy of prevention, detection and victim assistance. Stopping identity theft and refund fraud is a top priority for the IRS.

(3) Identity theft cases are among the most complex handled by the IRS. The IRS is continuously reviewing processes and policies to minimize the incidence of identity theft and to help those who find themselves victimized.

(4) In FY 2013, the IRS opted to develop specialized teams trained in identity theft case processing to handle the influx of tax-related identity theft cases.

25.23.1.1.2
(11-09-2020)
Terms/Definitions/ Acronyms

(1) **IMF Identity Theft-** A misrepresentation of the taxpayer's or dependent's identity that is committed or attempted, using a person's identifying information without authority. These are the types of IMF Identity Theft:

a. **Tax-Related Identity Theft:** A taxpayer's or dependent's personal information is used without their knowledge or permission to file a tax return

Example: The taxpayer attempts to file a tax return but is unable to because a tax return has already been filed using their Social Security Number (SSN) for the same period. The taxpayer has no knowledge of a tax return already on file.

Example: The dependent's legal guardian attempts to file a tax return but is unable to because their dependent's SSN has already been used on a tax return filed for the same period. The taxpayer has no knowledge of anyone else eligible to use that person as a dependent for tax purposes.

b. **Non-Tax-Related Identity Theft:** A taxpayer's or dependent's personal information has been compromised and used without their permission for purposes other than their tax administration

Example: The taxpayer validates that they have had their or their dependent's personal information compromised and used without their permission for purposes other than their tax administration, such as a credit card or bank account they did not authorize.

c. **Employment-Related Identity Theft:** The taxpayer's SSN and / or other personal information has been used to obtain or maintain employment. Their SSN may be used to report income on a Form W-2 which may result in an erroneous assessment of income. Employment related identity theft is considered "non-tax" related because it does not involve the filing of a fraudulent tax return. However, the income generated by the person using the SSN may have a tax account impact if it results in the assessment of additional tax if not identified and treated prior to the assessment.

Example: The taxpayer calls the IRS inquiring about a CP 2000 received by the taxpayer questioning income they have no knowledge of. After further research, the Contact Service Representative (CSR) determines the income in question is a result of income reported under the taxpayer's TIN. The taxpayer suspects he may be a victim of identity theft.

(2) **BMF Identity Theft-** Is defined as creating, using, or attempting to use a business' identifying information without authority to obtain tax benefits:

Example: **Identity Theft:** An identity thief files a business tax return (Form 1120, Form 720, etc.), using the Employer Identification Number (EIN) of an active or inactive business without the permission or knowledge of the EIN's owner, to obtain a fraudulent refund.

Example: **Identity Theft:** An identity thief, using the Employer Identification Number (EIN) of an active or inactive business without the permission or knowledge of the EIN's owner, files bogus Forms 941 and/or W-2s to support bogus Form(s) 1040 claiming a fraudulent refund.

Example: **Identity Theft:** An identity thief fraudulently obtains an EIN, using the name and SSN of another individual as the responsible party, without their approval or knowledge, to file fraudulent tax returns (Form 941, Form 1120, Form 1041, etc.), obtain a refund, or further perpetuate individual identity theft or refund fraud.

(3) **Determination of Identity Theft-** If the IMF or BMF taxpayer submits a valid claim or the IRS identifies an incident through an analysis of the taxpayer's account or from other sources, a determination is made that identity theft has

occurred. At that point, the Service should take an action on the taxpayer's account. For identity theft determination purposes, an "action on the account" refers to the placement of a tax or non-tax related identity theft indicator.

(4) **Preparer Misconduct**: Return preparer misconduct involves the orchestrated preparation and filing of false income tax returns (in either paper or electronic form), including Form 1040-X, by unscrupulous preparers who may change direct deposit information or claim, for example:

- Inflated personal or business expenses;
- False deductions;
- Unallowable credits;
- Excessive exemptions; or
- Fraudulent tax credits such as the Earned Income Tax Credit (EITC).

The preparer's clients may or may not have knowledge of the false expenses, deductions, exemptions and/or credits shown on their tax returns.

Example: A taxpayer used a preparer in 2015 to prepare and file Form 1040. The preparer changed the return by increasing the withholding tax claimed and diverted the resulting refund into the preparer's personal account. This is preparer misconduct. The AC 504 is input with an Return Preparer Misconduct (RPM) related MISC Code For cases involving return preparer misconduct, refer to IRM 25.24, Return Preparer Misconduct Program, for guidance.

Note: Refer to your functional IRM for guidance on resolving preparer misconduct cases.

(5) **Personally Identifiable Information (PII).** Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Safeguarding and preventing the unauthorized disclosure of PII is a responsibility that is shared by all Internal Revenue Service (IRS) employees and contractors. Lost or disclosed PII may be used to perpetrate identity theft or other forms of fraud if the information falls into unauthorized hands. The definition of personally identifiable information is provided by *OMB 07-16*. For further information about PII, see the *Personally Identifiable Information* page in the *Disclosure and Privacy Knowledge Base.*

(6) **Incident -** The term "incident" refers to an occurrence or event involving identity theft as it applies to a specific tax year(s) as reported by the taxpayer.

(7) **Data Breach -** is an unauthorized release of PII. Not all data breaches impose a risk to tax-related identity theft. For internal data breaches, refer to IRM 10.5.4.5, IRS Breach Tracking Indicator - Objectives.

(8) For a full listing of Identity Protection terms, see Exhibit 25.23.1-1, Glossary of Identity Protection Terms and Definition.

Note: For a more extensive list, see Exhibit 25.23.1-1 Glossary of Identity Protection Terms and Definitions

25.23.1.1.3
(09-19-2017)
Related Internal Revenue Manuals (IRM) and other Reference Materials

(1) Throughout IRM 25.23.1, Identity Protection and Victim Assistance - Policy Guidance, there are links/references to other IRMs for handling program specific issues.

(2) Employees/CSRs are responsible for familiarizing themselves with and utilizing all linked/referenced IRMs, as appropriate. This includes, but is not limited to sections, within the following:

- IRM 2, Information Technology
- IRM 3, Submission Processing
- IRM 4, Examining Process
- IRM 5, Collecting Process
- IRM 10.5, Security, Privacy and Assurance
- IRM 11.3, Disclosure of Official Information
- IRM 13, Taxpayer Advocate Service
- IRM 20, Penalty and Interest
- IRM 21, Customer Account Services
- IRM 25, Special Topics

In addition, this IRM links to these Identity Theft Victim Assistance (IDTVA) function specific IRMs

- IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing
- IRM 25.23.3, IMF Identity Protection Specialized Unit (IPSU) Paper Overview and Guidance
- IRM 25.23.4, IDTVA Paper Process
- IRM 25.23.9, BMF Identity Theft Processing
- IRM 25.23.10, Compliance Identity Theft Case Processing
- IRM 25.23.11, Business Master File (BMF) Identity Theft Procedures for Accounts Management
- IRM 25.23.12, IMF Identity Theft Toll-Free Guidance
- IRM 25.24.1, Return Preparer Misconduct Victim Assistance - General Overview
- IRM 25.24.2, Return Preparer Misconduct Victim Assistance Specialized Accounts Management Processing

25.23.1.2
(10-01-2022)
Wage and Investment - Accounts Management - Identity Protection Strategy and Oversight (IPSO)

(1) In FY 2015, the IRS opted to consolidate Identity Theft (IDT) Operations to improve accountability, efficiency, and timeliness. This organizational structure will provide unified leadership and improve program oversight.

(2) Identity theft creates a heavy financial and emotional toll on its victims and severely burdens our economy. The IRS is focused on prevention and assistance activities including a comprehensive approach to protecting taxpayer information. The IRS will enhance efforts through three primary goals:

- Victim Assistance
- Outreach
- Prevention

(3) **Wage and Investment (W&I) Identity Protection Strategy and Oversight (IPSO)** supports Servicewide efforts to recognize and resolve identity theft issues while striving to provide a uniform and consistent approach to victim assistance. IPSO maintains enterprise governance over identity protections and victim assistance.

(4) **Identity Protection (IP) Headquarters** is a headquarters operation that reports through the IPSO manager to Accounts Management leadership. The organization supports service wide Identity protection and victim assistance through:

- The development of short-term and long-term remedies to protect taxpayer information and make the experience of those who are already victims faster and more efficient.
- The development of Servicewide policy, procedures, and guidelines for the priority of recognizing, marking and acknowledging individual taxpayer claims involving identity theft.
- Support of IPSO activities within the scope of programs associated with identity protection.

(5) **Identity Theft Victim Assistance (ITVA) Headquarters** is a headquarters operation that reports through the IPSO manager to Accounts Management leadership. This organization supports the IDTVA organization through:

- The development of ITVA policy, procedures, and guidelines for resolving individual taxpayer accounts involving identity theft or return preparer misconduct.
- Support IPSO activities within the scope of programs associated with victim assistance.
- Evaluation of legislative changes in current policy decisions, process improvement suggestions, technical advice, and other sources to write or revise IRM procedures.
- Completion of reviews of IDTVA (IDT & RPM), and the IDT and TPP Toll-free operations to ensure victims or customers of those functions receive timely and accurate actions, identify trends, receive input on above stated guidance, make recommendations and resolving issues at the earliest possible point.

(6) **Identity Theft Victim Assistance (IDTVA)** is an organization that combines the skills of Accounts Management and Compliance within one organizational framework to resolve post-processing identity theft cases while focusing on the customer's experience. There are three major functional components of IDTVA:

- **IDTVA-Identity Protection Specialized Unit Inventory Program** - plays an integral role in daily operations. Inventories include: Processing non-tax-related identity theft claims (IDT4), Requests for copies of Fraudulent Tax Returns (IDT7), Applications for an IP PIN (IDTX) , and performing global review account reviews (GRVW).
- **IDTVA-Accounts (A)**- resolves tax-related identity theft cases discovered or reported in normal Accounts Management casework, such as duplicate filing conditions.
- **IDTVA Specialties** - resolves tax-related identity theft cases discovered or reported in normal Campus Compliance casework, such as replies to Exam, AUR, and ACS notices.

(7) The following Functions, which are responsible for publishing guidance to address/resolve incidents of IDT discovered in their processing, are not within the current framework of IDTVA:

- Appeals
- Criminal Investigation (CI)

- Combined Annual Wage Reporting (CAWR)
- Field Assistance
- Field Collection
- Field Exam
- Large Business and International (LBI)
- Return Integrity and Compliance Services (RICS) - Taxpayer Protection Program (TPP) and Integrity Verification Operations (IVO)
- Submission Processing (SP)

25.23.1.2.1
(09-17-2019)
Identity Protection (IP) Program Responsibilities

(1) IPSO maintains enterprise-wide identity protection program oversight. This includes internal outreach to all Business Operating Divisions to ensure the established policies are implemented and supported Servicewide.

(2) IPSO has the following specific responsibilities related to administering the Identity Protection Program in IRS:

a. Building programs to reduce incidents of identity theft such as the Identity Protection Personal Identification Number (IP PIN) and the identity theft unpostable process.
b. Defining, communicating, and assigning responsibility for the IRS' substantiated identity theft incident tracking program.
c. Raising taxpayer awareness of identity theft techniques through outreach.
d. Reducing taxpayer burden and improving service options while addressing and resolving identity theft cases.
e. Protecting Treasury revenue by identifying suspicious filings before the refunds are generated.
f. Increasing operational efficiency of the IRS by detecting and processing reported identity theft incidents as early and consistently as possible.
g. Identifying emerging trends and developing appropriate strategies and responses.
h. Developing, defining, monitoring, and executing identity theft policies and procedures.
i. Participating in risk assessments on IRS business processes, where appropriate.
j. Communicating and coordinating with both internal and external stakeholders (such as the Federal Trade Commission) to ensure consistency regarding identity theft issues.
k. Determining identity theft performance measures to assess the effectiveness of the program and identity theft initiatives throughout the IRS and making recommendations for improvement as appropriate.
l. Overseeing the maintenance, publication, and conveyance of the Servicewide identity theft guidance via the Identity Protection and Victim Assistance Internal Revenue Manual (IRM), ensuring that the information contained remains current.
m. Conducting identity theft program reviews, which include, but are not limited to: IRM reviews to verify procedural consistency; and closed case reviews to ensure adherence to Servicewide policies and procedures.
n. Evaluating new technologies and assessing benefits for use in identity theft initiatives.

25.23.1.2.2
(09-22-2016)
Identity Theft Victim Assistance (ITVA)-Program Responsibilities

(1) The mission of Identity Theft Victim Assistance (ITVA) is to develop policy, procedures, and guidelines for resolving individual taxpayer accounts upon contact from a victim of identity theft (IDT) or Return Preparer Misconduct (RPM). ITVA issues guidance for:

- Researching accounts based on a return or claim from an apparent victim
- Correcting accounts when IDT or RPM is substantiated, and
- Communicating with victims

(2) To accomplish the mission, ITVA:

- Supports all activities identified by Identity Protection Strategy and Oversight (IPSO) with specific purview of programs associated with victim assistance.
- Evaluates legislative changes, current policy decisions, process improvement suggestions, technical advice, and other sources to write or revise IRM procedures.

(3) IDTVA employees are located at various campus locations. Refer to IRM 25.23.4, IDTVA Paper Process, for IDTVA campus locations and groups.

25.23.1.3
(09-07-2021)
Identity Theft and the IRS

(1) Identity theft occurs when someone uses an individual's personal information, such as name, SSN, or other identifying information without permission or knowledge, to commit fraud or other crimes.

(2) For the purpose of victim assistance, there are two types of Identity Theft:

- Identity Theft in Tax Administration, or Tax-Related Identity Theft; Identity theft with a direct effect on the taxpayer's filing and payment requirements, such as their ability to file a tax return, receive a refund or take other actions associated with these responsibilities. Tax-related identity theft is most often associated with the theft of a taxpayer's SSN (see IRM 25.23.1.3.1, Identity Theft in Tax Administration, below).
- Non-Tax-Related Identity Theft: The taxpayer experiences an incident, such as becoming a victim of a data breach from their medical office or a lost wallet or stolen purse - which may place them at risk of identity theft related to their credit or finances - but there is no direct effect on tax administration at that time.

(3) Taxpayers may notify the IRS when they believe they have experienced an identity theft incident. In these instances, taxpayers must make a claim, and in some cases, provide additional information to establish that they are identity theft victims.

(4) Identity theft often leaves its victims feeling helpless and distraught. Service employees should exercise empathy in dealing with victims. Refer to IRM 25.23.2.2.1 Taxpayer Interaction, for additional information. The Taxpayer Bill of Rights (TBOR), lists rights that already existed in the tax code, putting them in simple language and grouping them into 10 fundamental rights. Employees are responsible for being familiar with and acting in accord with taxpayer rights. See IRC 7803(a)(3)Execution of Duties in Accord with Taxpayer Rights. For additional information about the TBOR, see *http://www.irs.gov/taxpayer-bill of rights*

(5) Identity theft cases will be prioritized and worked expeditiously.

25.23.1.3.1
(09-22-2016)
Identity Theft in Tax Administration

(1) Tax-Related Identity theft can affect tax administration in three primary ways:

- **Employment or Income Related** - This occurs when the identity thief uses the victim's SSN to obtain employment, resulting in what may appear as unreported income under the victim's account.
- **Refund Related** - This occurs when the identity thief uses the victim's SSN to file a false federal income tax return to obtain a refund (or Economic Impact Payment (EIP)). If the thief files before the victim, the victim may not receive his or her refund within a reasonable time frame.
- **Business Related** Business Master File (BMF) identity theft is defined as creating, using or attempting to use a business's identifying information, without authority, to obtain tax benefits.

25.23.1.4
(11-01-2018)
IRS Employees Who May be Victims of Tax-Related Identity Theft

(1) IRS employees who believe they may be victims of tax related identity theft should take the following actions:

- File Form 14039, Identity Theft Affidavit;

  Note: Be sure to write legibly and follow the instructions on the form.
- Contact your local Treasury Inspector General for Tax Administration (TIGTA) office immediately, in person or by phone at 800-366-4484;
- Call the number on the notice as soon as possible, if you receive an IRS notice that makes you think you have become a victim of tax-related identity theft;
- Contact TIGTA immediately, if you believe someone is using your information to impersonate an IRS employee, or if you suspect an IRS employee may be involved in your identity theft;
- Visit *Identity Theft Central* and IRM 25.23.2.2.1, Taxpayer Interaction, for additional information and resources.

Reminder: If an employee's tax account is accessed, Form 11377, Taxpayer Data Access, must be completed and submitted.

25.23.1.4.1
(03-31-2016)
IRS Employees Who May be Victims of Non-Tax-Related Identity Theft

(1) IRS employees who believe they may be victims of non-tax related identity theft should take the following actions:

- Obtain an IP PIN online at *GETANIPPIN.gov*
- You will need to file Form 14039, Identity Theft Affidavit.

  Note: Be sure to write legibly and follow the instructions on the form.

Reminder: If an employee's tax account is accessed, Form 11377, Taxpayer Data Access, must be completed and submitted.

25.23.1.5
(09-17-2019)
Identity Protection and Victim Assistance Initiatives

(1) The IRS established and expanded initiatives to address identity theft in tax administration which includes:

- Identity Theft Training

25.23.1.5.1
(03-04-2020)
Awareness Training and Education

(1) IPSO maintains the annual employee awareness training.

(2) Presently IPSO maintains two Integrated Talent Management (ITM) courses:

- **Identity Theft Awareness Briefing (ITM Course Number 43113)** – is designed for new IRS employees, or those newly appointed to positions, that have direct contact with taxpayers - especially those who are or may become victims of identity theft. This course may also be used by anyone who wants to learn more about identity theft. It is intended to give guidance regarding such topics as IRS initiatives to combat identity theft, empathy for the taxpayer seeking assistance, the IP PIN program, identity theft indicators and includes internal and external resources.
- **Identity Protection Overview (ITM Course Number 56188)** – is designed for seasoned employees. This is a streamlined briefing for employees who have taken the full Identity Theft Awareness Briefing (43113). It shares high-level information and contains updates to identity theft programs and initiatives. This training is for more experienced employees who no longer require the in-depth training offered by the Identity Theft Awareness Briefing.

Employees are required to certify the required courses are completed.

(3) Accounts Management (AM) Headquarters Functional Training coordinators provide annual Continuing Professional Education (CPE) for IDTVA employees.

25.23.1.5.2
(09-18-2020)
Guidance to Implement Section 1402 of the Taxpayer First Act

(1) Pursuant to Internal Revenue Code (IRC) 7526, subject to the availability of appropriated funds, the IRS may award matching grants for the development, expansion, or continuation of Low-Income Taxpayer Clinics (LITCs). LITCs are programs that provide representation to low income taxpayers for free or a nominal fee to assist them in resolving concerns with the IRS. In addition, LITCs provide education and outreach for taxpayers who speak English as a second language.

(2) Section 1402 of the Taxpayer First Act changed existing law, rulings, and regulations to allow IRS employees to refer a taxpayer to an LITC site without violating the applicable standards of ethical conduct. Thus, IRS employees can direct a taxpayer to a particular LITC and are encouraged to do so when it appears a taxpayer might be eligible and could benefit from LITC assistance.

(3) Publication 4134, Low Income Taxpayer Clinic List, provides information to taxpayers about accessing LITCs and lists locations by state. LITCs are independent from the Internal Revenue Service (IRS) and the Taxpayer Advocate Service (TAS). LITCs represent individuals whose income is below a certain level and who need to resolve tax problems with the IRS. LITCs can represent taxpayers in audits, appeals, and tax collection disputes before the IRS and in court. In addition, LITCs can provide information about taxpayer rights and responsibilities in different languages for individuals who speak English as a second language. Services are offered for free or a small fee. For more information or to find an LITC, see the LITC page at *www.taxpayeradvocate.irs.gov/litcmap* or IRS Publication 4134, Low Income Taxpayer Clinic List. Taxpayers can access this publication online at *www.irs.gov/forms-pubs* or by calling the IRS toll-free at 800-829-3676.

(4) Employees may:

a. advise taxpayers of the availability of, and eligibility requirements for receiving, advice and assistance from one or more specific qualified low-income taxpayer clinics receiving funding under this section, and;
b. provide information regarding the location of, and contact information for, such clinics.

25.23.1.6
(09-19-2017)
Data Breach - Business Entities Whose Employees or Clients PII was Breached

(1) Businesses, hospitals, doctor's offices, etc., may contact IRS when their employee or client PII has been breached. State or Local Law Enforcement, or any other third party such as tax practitioners, accountants, etc., attempting to assist an entity that was breached may also contact IRS. If you are contacted by one of these entities, and they are seeking guidance for their employees/clients, the following actions/precautions should be recommended to the breached entity/third party so they may alert the affected individuals/clients/employees whose data was breached to take the following precautions:

- Contact the Federal Trade Commission (FTC) Identity Theft Hotline at 877-438-4338, establish an account with Social Security Administration (SSA) to review earnings records; and contact one of the three major credit bureaus: Equifax at 800-525-6285, Experian at 888-397-3742, or TransUnion at 800-680-7289; and
- Obtain an IP PIN online at *GETANIPPIN.gov*
- Not every data breach results in identity theft, and not every identity theft is tax-related identity theft. If the individual/client whose PII was breached received IRS correspondence or their e-file tax return was rejected as a duplicate (and the taxpayer did not file that return), the individual/client may take these additional steps with the IRS:

- Continue to file their tax return, even if they must do so by paper, and attach the Form 14039
- Watch for any follow-up correspondence from the IRS and respond quickly

Note: The affected individuals will need to file Form 14039 to have their account protected as the IRS does not accept Form 14039 from unauthorized third parties.

(2) If you are contacted by a tax return preparer reporting a theft in their office that could lead to a data breach, instruct them to report client data theft to their local stakeholder liaison. Refer to *https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts-1* for contact information. Liaisons will notify IRS Criminal Investigation and others within the agency on their behalf. Speed is critical. If reported quickly, the IRS can take steps to block fraudulent returns in their clients' names.

(3) If you are contacted by a business or payroll service provider reporting a data loss relating to W2 information, instruct them to visit *https://www.irs.gov/individuals/form-w2-ssn-data-theft-information-for-businesses-and-payroll-service-providers*

(4) For additional information on identity theft guidance, refer to IRM 25.23.12, IMF Identity Theft Toll-Free Guidance.

25.23.1.7
(09-18-2020)
Taxpayers who are Victims of a Data Breach

(1) Taxpayers may contact IRS when a business, employer, or financial institution alerts them that their PII was breached. Take the following actions dependent upon the facts and circumstances of the taxpayer's accounts (tax-related or non-tax related):

Caution: Not all data breaches lead to identity theft and not all identity theft is tax-related identity theft.

(2) **No Tax-Related Issues**: CSRs will provide the following information to taxpayers who identify themselves as data breach victims and who have no tax-related issues:

- Obtain an IP PIN online at *GETANIPPIN.gov*
- Stay informed about the steps being taken by the breached entity;
- Follow the Federal Trade Commission recommended steps, including:

- Notify one of the three major credit bureaus to place a fraud alert on your credit file;
- Close any accounts opened without your permission;
- Visit *www.identitytheft.gov* for additional guidance.

Note: For IDT victims experiencing a tax-related IDT incident and a Form 14039 should be filed, the FTC website provides an IRS authorized fillable Form 14039. This was intended to consolidate and relieve the overall process for self-reporting.

(3) **Tax-Related Issues**: Advise the taxpayer to file Form 14039, Identity Theft Affidavit if:

- The IRS has informed the taxpayer they were victims of an identity theft tax fraud.
- The taxpayer's e-file return was rejected as a duplicate.

Note: For victims needing to complete Form 14039, in addition to the fillable IRS Form 14039 on IRS.gov, the FTC has a fillable Form 14039 on *www.identitytheft.gov* This is authorized by the IRS and its placement on the FTC site is intended to consolidate and relieve the overall self-reporting and recovery burden of victims who are reporting their situation to the FTC and who intend to also complete an IRS Form 14039.

For additional information refer to 25.23.2.3 Identity Theft Claims – General Guidelines.

(4) For information on specific breach incidents and definitions of the various IDT indicators and MISC codes, see IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing

This Page Intentionally Left Blank

Exhibit 25.23.1-1 (10-01-2022)
Glossary of Identity Protection Terms and Definitions

Access - The ability or opportunity to gain knowledge of personally identifiable information.
Breach - The loss of control, disclosure, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than the authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Determination of Identity Theft- If the IMF or BMF taxpayer submits a valid claim or the IRS identifies an incident through an analysis of the taxpayer's account or from other sources, a determination is made that identity theft has occurred. At that point, the Service should take an action on the taxpayer's account. For identity theft determination purposes, An "action on the account" refers to the placement of a tax or non-tax related identity theft indicator.
Employment Related Identity Theft - occurs when someone, other than the valid SSN owner, uses the SSN to obtain or retain employment. Employment Related Identity Theft is considered "non-tax" related because it does not involve the filing of a fraudulent return. However, income generated by a person other than the valid SSN owner may result in the assessment of additional tax if not addressed prior to the assessment.
Federal Trade Commission (FTC) - An independent agency of the United States government, established in 1914 by the Federal Trade Commission Act, with the principal mission of promoting "consumer protection" and the elimination and prevention of what regulators perceive to be "anti-competitive" business practices.
Harm - Includes any of the following effects of a breach of confidentiality, integrity, availability, or fiduciary responsibility: • Potential for blackmail; • Disclosure of private facts; • Mental pain and emotional distress; • Potential for secondary uses of the information that could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem; • Identity theft; or • Financial loss
Identity Theft - A fraud that is committed or attempted, using a person's identifying information without authority. • **Tax Related Identity Theft**- Identity Theft that impacts individual or business Federal tax accounts. • **Non-tax Related Identity Theft** - Identity theft that does not impact individual or business Federal tax accounts, such as; lost wallet/purse, breach of personal data, questionable credit activity.
Identity Theft Claim -refers to any combination of: • Form 14039, or • Police report, or • For other than Compliance functions, a written statement from the taxpayer indicating they are or maybe victim of identity theft. ***Note:*** Cases that are referred to IDTVA from a Compliance function must include a Form 14039 or police report to be considered an Identity Theft claim.

Exhibit 25.23.1-1 (Cont. 1) (10-01-2022)
Glossary of Identity Protection Terms and Definitions

Identity Theft Liaison - A listing of individuals in the business units that are the contacts for the W&I AM IPSU, when IDTVA-I (IPSU) sends Form 14027-B, Identity Theft Case Referral, for monitoring account activity on cases with open controls. A current listing of "ID Theft Liaisons (Functional)" can be found on SERP under the Who/Where Tab.
Identity Theft Assistance Request (ITAR) Liaison - A listing of individuals in the business units that are the contacts for the W&I AM IDTVA. A current listing of "ID Theft Liaisons (Functional)" can be found on SERP under the Who/Where tab.
Incident - For the purpose of this IRM, the term "incident" refers to an occurrence or event involving identity theft as it applies to a specific tax year(s) as reported by the taxpayer.
Incident Management - The process of managing incidents involving the loss or disclosure of data.
Information Technology - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.
Loss - Any event where an item is misplaced and/or neither the official owner nor the intended recipient has possession of the item in the expected time frame. A loss may involve an IRS-owned physical asset such as a laptop, blackberry, cell phone, and/or other portable media, or electronic or hard copy data that may contain Sensitive But Unclassified (SBU) data or Personally Identifiable Information (PII) such as paper or electronic taxpayer records, personnel records, or other identifying data, or a combination of a physical asset and electronic and/or hard copy data.
Office of Management and Budget (OMB) - A cabinet-level office that oversees the activities of federal agencies and monitors the adherence of their assigned federal programs to presidential policies.
Personally Identifiable Information (PII) - The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, SSN, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Please see *OMB 07-16*. For further information about PII, see the *Personally Identifiable Information* page in the *Disclosure and Privacy Knowledge Base.*
Risk - The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security and privacy controls that would mitigate this impact.
Safeguards - Protective measures prescribed to meet the privacy requirements specified for an information system.
Unpostable- A transaction which cannot be posted to a taxpayer's account because the transaction failed certain Master File validation checks.

Exhibit 25.23.1-2 (09-19-2017)
References

The Identity Protection Strategy & Oversight was established to ensure Servicewide implementation of federal directives to protect citizens and government employees. The following are the principal documents involving the Identity Protection Program:

OMB Memoranda

1. *M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006*
2. *M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003*

OMB Memoranda are available at Office of Management and Budget at *http://www.whitehouse.gov/omb/memoranda.*

Other Federal Guidance

1. Combating Identity Theft: A Strategic Plan, The President's Identity Theft Task Force Report, April 2007
2. Combating Identity Theft, Volume II: Supplemental Information, The President's Identity Theft Task Force Report, April 2007
3. President's Identity Theft Task Force Report Summary of Interim Recommendations, September 2006
4. IRM 1.2.1.17.1, Policy Statement 10–1 (formerly P-25-1), Assisting taxpayers who report they are victims of identity theft

The President's Identity Theft Task Force documents are available at *http://www.ftc.gov* and *http://www.justice.gov*

Identity Protection Victim Assistance Internal Revenue Manuals

- IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing
- IRM 25.23.3, IMF Identity Protection Specialized Unit (IPSU) Paper Overview and Guidance
- IRM 25.23.4, IDTVA Paper Process
- IRM 25.23.9, BMF Identity Theft Processing
- IRM 25.23.10, Compliance Identity Theft Case Processing
- IRM 25.23.11, Business Master File (BMF) Identity Theft Procedures for Accounts Management
- IRM 25.23.12, IMF Identity Theft Toll-Free Guidance
- IRM 25.24.1, Return Preparer Misconduct Victim Assistance - General Overview
- IRM 25.24.2, Return Preparer Misconduct Victim Assistance Specialized Accounts Management Processing