



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

5.1.28

MARCH 24, 2023

## EFFECTIVE DATE

(03-24-2023)

## PURPOSE

- (1) This transmits revised IRM 5.1.28, Field Collection Procedures, Identity Theft for Collection Employees.

## MATERIAL CHANGES

- (1) Refer to the table below for details on the list of material changes in this IRM.

IRM Subsection	Description of Change
IRM 5.1.28.1.6	Added additional acronyms.
IRM 5.1.28.1.7	Added a new paragraph (2) to the Collection Procedures Knowledge Base (KB) to assist collection employees in understanding and applying identity theft procedures.
IRM 5.1.28.2	Removed paragraph (4) note in reference to when referring TAS referrals to IPSU.
IRM 5.1.28.5.1	Added a new paragraph (4) to include procedures for addressing the unpostable return.
IRM 5.1.28.8.4	Modified title to clarify that this subsection covers IMF tax-related identity theft.
IRM 5.1.28.8.4 (IPU 22U0567 issued 04-28-2022)	Updated paragraph (2)a to correct the Kansas City - IDTVA-A ACSS fax number.
IRM 5.1.28.8.4	Removed note in paragraph (3) as it no longer applies.
IRM 5.1.28.12	Added an IRM reference in paragraph (3)a to refer to suits to recover erroneous refunds.
IRM 5.1.28.13.2	Added a note under paragraph (7) to ensure to perform extensive research to support an identity theft determination or eliminate a routine account issue.
IRM 5.1.28.14.1	Revised title of the IRM subsection to identify where to route and process the input of BMF identity theft codes. Added table to paragraph (1) to provide DITA contact information.

<b>IRM Subsection</b>	<b>Description of Change</b>
IRM 5.1.28.16	Revised paragraph (2) to reference the new SERP identity theft webpage when searching for contact information related to field collection and OIC casework.
IRM 5.1.28.16	Added a note under paragraph (3) on how to seek assistance when the collection employee and/or group manager encounters a complex identity theft issue that is not found within the IRM, or there is an adjustment issue that needs to be addressed.
IRM 5.1.28.16.1	Revised the “If/Then” table under paragraph (1) to change the referral procedures involving BMF identity theft is completed on Form 14566, BMF Identity Theft Referral and routed through the appropriate area ID theft liaison to the SBSE ID theft liaison - collection policy.
IRM 5.1.28.16.1	Updated the text in paragraphs (3) and (4) when completing Form 3870 to capture required information when a referral to another function is needed.
IRM 5.1.28.16.3	Revised the “If/Then” table under paragraph (1) to change the referral procedures involving BMF identity theft is completed on Form 14566, BMF Identity Theft Referral, and the form is forwarded to the area identity theft liaison for review.
Throughout	Editorial changes were made to update links and reference points and clarify information to assist and support the end-user.
Throughout	Replaced the words “he”, “she”, “his” and “her” with gender-neutral language.

## EFFECT ON OTHER DOCUMENTS

This material supersedes IRM 5.1.28 dated July 14, 2021. The following IRM Procedural Update (IPU) has been incorporated into this IRM: IPU 22U0567 issued 04-28-2022.

## AUDIENCE

Revenue officers and other caseworkers in SB/SE Collection

Kareem Williams  
Director, Collection Policy  
Small Business/Self-Employed

5.1.28

Identity Theft for Collection Employees

## Table of Contents

5.1.28.1 Program Scope and Objectives

5.1.28.1.1 Background

5.1.28.1.2 Authority

5.1.28.1.3 Responsibilities

5.1.28.1.4 Program Management and Review

5.1.28.1.5 Program Controls

5.1.28.1.6 Terms/Definitions/Acronyms

5.1.28.1.7 Related Resources

5.1.28.2 Taxpayer Interaction

5.1.28.3 Identity Theft and Disclosure

5.1.28.3.1 Tax Return Filed

5.1.28.3.2 Tax Return Information - Refund Fraud

5.1.28.3.3 Tax Return Information - Forms W-2 and 1099

5.1.28.3.4 Victim Disclosure

5.1.28.3.5 Employer Disclosure

5.1.28.4 Collection Activity in Identity Theft Cases

5.1.28.4.1 Assessment is Result of Identity Theft

5.1.28.4.1.1 Returning Levied Property in Cases of Identity Theft

5.1.28.4.1.2 Returning Accounts to Currently not Collectible Status

5.1.28.4.1.3 Returning Accounts to Installment Agreement Status

5.1.28.5 Types of IMF Identity Theft

5.1.28.5.1 IMF Identity Theft (Revenue Protection) Return with Unpostable Code (UPC 126, MFT 32)

5.1.28.6 Standard IMF Tax Related Identity Theft Claim Requirements

5.1.28.6.1 When to Request Additional Information to Support Claim/Allegation of Identity Theft

5.1.28.6.2 Acknowledging and Handling IMF Identity Theft Claim

5.1.28.7 Making an Identity Theft Determination

5.1.28.7.1 Validating Claim of Identity Theft for Fraudulent Filing Purposes

5.1.28.7.2 Validating Claim of Identity Theft for Employment Purposes

5.1.28.8 Identity Theft Case Resolution

5.1.28.8.1 Individual Taxpayer Alleged Identity Theft vs. IRS Identified Identity Theft

5.1.28.8.2 Individual Taxpayer Alleges Identity Theft

5.1.28.8.3 IRS Identified Identity Theft

5.1.28.8.4 Form 3870 Preparation and Routing of IMF Tax-Related Identity Theft

5.1.28.8.5 IMF Identity Theft Indicator Codes

5.1.28.8.5.1 Identity Theft Action Code Input Procedures

- 5.1.28.8.5.2 Completion of Form 4844
- 5.1.28.8.5.3 Miscellaneous Fields
- 5.1.28.8.5.4 Secondary Date Field
- 5.1.28.8.5.5 Remarks Block
- 5.1.28.8.6 Identity Theft Code TC 971 AC 522 Reversal Procedures (TC 972 AC 522)
- 5.1.28.8.7 Identity Theft Code TC 971 AC 501 and AC 506 Reversal Procedures
  - 5.1.28.8.7.1 Secondary Date Field — TC 972
- 5.1.28.9 Taxpayer is Not a Victim of Identity Theft
- 5.1.28.10 Taxpayer Committed Identity Theft for Purposes of Tax Evasion
- 5.1.28.11 Compliance Against Persons Using Another Person's SSN for Employment
- 5.1.28.12 Erroneous Identity Theft Refund Issued to Victim
- 5.1.28.13 BMF Identity Theft
  - 5.1.28.13.1 Types of BMF Identity Theft Processing
  - 5.1.28.13.2 Research to Substantiate BMF Identity Theft
- 5.1.28.14 BMF Identity Theft Tracking Indicators
  - 5.1.28.14.1 BMF Identity Theft Action Code is Routed and Processed on Form 4844
    - 5.1.28.14.1.1 Miscellaneous Field Input
    - 5.1.28.14.1.2 Secondary Date Field
  - 5.1.28.14.2 Reversing Pending BMF Identity Theft Indicators
- 5.1.28.15 BMF Taxpayer Identity Theft Claim
- 5.1.28.16 BMF Identity Theft Case Actions
  - 5.1.28.16.1 Form 941/944 Balance Dues
    - 5.1.28.16.1.1 Researching Issued Refunds
  - 5.1.28.16.2 BMF Bal Dues - Taxpayer's Name and SSN Used by Third Party
  - 5.1.28.16.3 Business Tax Return Claiming Refundable Credit
- 5.1.28.17 Form 14566, BMF Identity Theft Referral

Exhibits

- 5.1.28-1 IMF Form 4844 Example Input of TC 971 AC 522 Pending Claim
- 5.1.28-2 IMF Form 4844 Example Input of TC 972 AC 522 No Identity Theft
- 5.1.28-3 BMF Form 4844 Example Input of TC 971 AC 522 Initial Allegation or Suspicion of Identity Theft
- 5.1.28-4 BMF Form 4844 Example Input of TC 971 AC 522 Indicator Case Resolved
- 5.1.28-5 IDRS Research - Taxpayer Never Applied for an EIN
- 5.1.28-6 IDRS Research - Active Business
- 5.1.28-7 IDRS Research - Inactive Business

5.1.28.1  
(07-14-2021)  
**Program Scope and Objectives**

- (1) **Purpose.** This section discusses the overall identity theft guidance, processes, and procedures aimed at preventing identity theft, protecting taxpayers, and providing assistance to victims of identity theft. While many topics are touched upon in this section, comprehensive guidance about all of them cannot be included here. As you use this section, remain alert for references to other resources, such as related IRMs and websites. Access that guidance as needed, to ensure a thorough understanding of topics. Subsections within this section are:
  - Establish procedures for taxpayer interaction.
  - Define disclosure steps in identity theft cases.
  - Define collection activity in identity theft cases.
  - Identify types of identity theft cases.
  - Discuss identity theft claim requirements.
  - Describe steps needed in determining identity theft cases.
  - Describe steps needed to resolve identity theft cases.
- (2) **Audience.** These procedures and guidance apply to IRS Field Collection revenue officers and group managers.
- (3) **Policy Owner.** Director, Collection Policy, SBSE.
- (4) **Program Owner.** Collection Policy, SBSE, Case Resolution Alternatives (CRA).
- (5) **Primary Stakeholders.** The primary stakeholders that are impacted by this IRM include:
  - Field Collection
  - Identity Protection Strategy and Oversight (IPSO)
  - Identity Theft Victim Assistance (IDTVA)
  - Designated Identity Theft Adjustment (DITA)
- (6) **Program Goals.** Identity theft places a burden on its victims and presents a challenge to businesses, organizations, and government agencies, including the Internal Revenue Service. By following the direction in this IRM section, employees can combat tax-related identity theft with an aggressive strategy for prevention, detection, and victim assistance.

5.1.28.1.1  
(07-14-2021)  
**Background**

- (1) The definitions for Individual Master File (IMF) and Business Master File (BMF) identity theft are:
  - IMF identity theft is the filing of an individual tax return when someone uses an individual's personal information, such as name, Social Security Number (SSN), or other identifying information without permission to obtain tax benefits, or cause taxpayer harm or to commit fraud or other criminal acts.
  - BMF identity theft is the filing of a business tax return when someone creates, uses, or attempts to use a business's or individual's identifying information without authority to obtain tax benefits or to enable fraudulent schemes.

5.1.28.1.2  
(03-24-2023)

**Authority**

- (1) The Identity Protection Strategy & Oversight Program was established to ensure servicewide implementation of federal directives to protect citizens and government employees. The following are the principal documents involving the identity theft program:

- Combating identity theft: A Strategic Plan, The President's Identity Theft Task Force Report, April 2007
- Combating identity theft, Volume II: Supplemental Information, The President's Identity Theft Task Force Report, April 2007
- President's Identity Theft Task Force Report Summary of Interim Recommendations, September 2006
- Office of Management and Budget (OMB), M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017 - [https://www.whitehouse.gov/wp-content/uploads/legacy\\_drupal\\_files/omb/memoranda/2017/m-17-12\\_0.pdf](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf)
- Office of Management and Budget (OMB), M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003 - <https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf>

5.1.28.1.3  
(07-14-2021)

**Responsibilities**

- (1) The Director, Collection Policy is the executive responsible for the policies and procedures related to W&I's identity theft program. They are responsible for overseeing program coordination for field collection personnel related to the identity theft program.
- (2) The program manager, Case Resolution Alternatives (CRA), is responsible for the delivery of policies and procedures put forward by the W&I identity theft program.
- (3) Field collection group managers and territory managers are responsible for ensuring the guidance and procedures described in this IRM are complied with.

5.1.28.1.4  
(07-14-2021)

**Program Management and Review**

- (1) **Program Effectiveness.** The program effectiveness is measured by the following review types and by level of management.
- Managers, leads, and on-the-job instructors (OJIs) use the Embedded Quality Review System (EQRS)/National Quality Review System (NQRS) Data Collection Instrument (DCI) to input case reviews. EQRS is used to evaluate employee performance and provide feedback and NQRS is used to ensure program delivery with this IRM. NQRS data is used to report the official organizational business quality results.
  - Case reviews are conducted by group managers to ensure compliance with this IRM.
  - Operational reviews are conducted by territory managers and area directors annually to evaluate program delivery and conformance to administrative and compliance requirements.

5.1.28.1.5  
(07-14-2021)  
**Program Controls**

- (1) Identity theft indicators. These indicators are utilized to track identity theft cases from the time a victim or IRS initially suspects identity theft through case closure. Identity theft indicators are posted as TC 971 AC 50X or TC 971 52X. Identity theft cases involving a BMF entity are input on the identified modules in CC TXMODA, and identity theft cases involving an IMF entity are posted on the entity (CC ENMOD).
- (2) Tax administration source codes. These source codes are utilized to track identity theft cases when they are initially identified. The tax administration source codes are shown with TC 971 AC 52X to identify the claim and your research results.

5.1.28.1.6  
(03-24-2023)  
**Terms/Definitions/Acronyms**

- (1) Frequently used terms within this IRM section, along with their definition, include:
  - a. **Tax-related identity theft:** Identity theft with a direct effect on the taxpayer's (or dependent's) or business'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 (or dependent's) Social Security number (SSN).
  - b. **Non-tax-related identity theft:** The taxpayer (or dependent) or business experiences an incident, such as becoming a victim of a data breach from their medical office or a lost wallet, a stolen purse, an online phishing scam or computer hack, which may place them at risk of identity theft related to their credit or finances. Still, there is no direct effect on tax administration at this time.
- (2) This table lists commonly used acronyms and their definitions within this IRM.

Acronym	Definition
AMS	Accounts Management System
BMF	Business Master File
BOD	Business Operating Division/ Function
CC	Command code
CII	Correspondence Imaging Inventory
CIS	Collection Information Statement
CLSIDT	BMF identity theft case resolved
CRA	Case Resolution Alternatives
DCI	Data Collection Instrument
DITA	Designated Identity Theft Adjust- ment
EQRS	Embedded Quality Review System

Acronym	Definition
FC	Field Collection
IDTVA	Identity Theft Victim Assistance
IDT	Identity theft
IDTCLM	Initial allegation or suspicion of identity theft prior to submitting claim (Form 14039 or Form 14039-B).
IDTDOC	When taxpayer provides and submits legible claim.
IMF	Individual Master File
INCMUL	Both income and MULTFL
IPSO	Identity Protection Strategy and Oversight
IRSID	IRS Initiated Suspicion of identity theft
MULTFL	Two or more returns filed under same SSN for the same tax period.
NFTL	Notice of Federal Tax Lien
NOFR	Taxpayer not required to file
NOIDT	Identity theft did not occur
NORPLY	Taxpayer did not provide supporting documents.
NQRS	National Quality Review System
OMB	Office of Management and Budget
PNDCLM	Taxpayer makes allegation of identity theft but has not yet provided their claim.
SB	Small Business & Self Employed
SERP	Servicewide Electronic Research Program
SSN	Social Security Number
TPI	Total Positive Income

5.1.28.1.7  
(06-20-2017)

#### Related Resources

(1) **IRM Resources:**

- IRM 25.23.1, Identity Protection and Victim Assistance - Policy Guidance

- IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing
- IRM 25.23.9, BMF Identity Theft Processing

(2) **Web Resource:**

- Identity Theft Procedures and Guidance: <https://portal.ds.irsnet.gov/sites/v1131/lists/identitytheftprocedures/landingview.aspx>

5.1.28.2  
(03-24-2023)  
**Taxpayer Interaction**

- (1) All taxpayers need to know that they have the right to prompt, courteous and professional service in their dealings with the IRS, to be spoken to in a way they can easily understand, to receive clear and easily understandable communications from the IRS, and to speak to a supervisor about inadequate service. For additional information about The Taxpayer Bill of Rights (TBOR), refer to the note below.
- (2) Taxpayers who have experienced identity theft are already victims, either emotionally and/or financially. Be aware of the impact and handle the contact with an additional level of sensitivity and understanding. Collection personnel must also guard against unauthorized disclosure and take steps to verify the identity of the taxpayer or tax practitioner.

**Note:** 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 TBOR, see <https://www.irs.gov/taxpayer-bill-of-rights> and IRM 1.2.1.2.36, Policy Statement 1-236.

- (3) In addition to providing the taxpayer with courteous service, educate the taxpayer about how to protect themselves and where to find additional information. Advise them to do the following:
  - Contact the Federal Trade Commission (FTC) to report identity theft
  - Contact the Social Security Administration (SSA) to report fraudulent activity
  - File a report with their local or state police
  - Contact their state Attorney General's office
  - Contact one of the three major credit bureaus: Equifax, Experian, or TransUnion
  - File Form 14039, Identity Theft Affidavit, or Form 14039-B, Business Identity Theft Affidavit, with the IRS if the identity theft affects tax administration
  - Review Pub 5027, Identity Theft Information for Taxpayers; and
  - Review the IRS website, <http://www.irs.gov/>, keyword "Identity Theft" or "ID Theft."
- (4) Refer taxpayers who claim financial hardship as a result of a tax-related identity theft issue to the Taxpayer Advocate Service (TAS) when TAS criteria is met, see IRM 13.1.7, Taxpayer Advocate Case Processing, Taxpayer Advocate Service (TAS) Case Criteria. Taxpayers meeting TAS criteria will be referred to TAS unless the IRS can provide relief or take substantive action towards providing relief on the same day. The definition of "same day" is within 24 hours. "Same day" cases include cases that can be completely resolved in

24 hours as well as cases in which you have taken steps to begin resolving the taxpayer's issues. Do not refer same day cases to TAS unless the taxpayer asks to be transferred to TAS and the case meets TAS criteria, see IRM 13.1.7.6, Same Day Resolution by Operations. Use Form 911, Request for Taxpayer Advocate Service Assistance (And Application for Taxpayer Assistance order), to refer cases meeting the criteria to TAS. If the taxpayer requests to contact TAS directly, advise the taxpayer to call 1-877-777-4778 toll-free, or go to <http://www.taxpayeradvocate.irs.gov/>.

5.1.28.3  
(05-15-2014)  
**Identity Theft and Disclosure**

- (1) IRC 6103(a) provides that tax returns and tax return information are confidential and are not to be disclosed except as authorized. See IRM 5.1.22, Field Collecting Procedures, Disclosure.

5.1.28.3.1  
(07-14-2021)  
**Tax Return Filed**

- (1) Per IRC 6103(b)(1) - The term "return" means any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed.
- (2) An income tax return fabricated by an identity thief, where the thief fraudulently acquires and uses another taxpayer's name and SSN for purposes of obtaining a fraudulent refund, is not a valid return. Moreover, such a return is not properly signed by the taxpayer in whose name the return is filed and, accordingly, lacks a valid signature.
- (3) A Form 1099, Miscellaneous Income and/or Form W-2, Wage and Tax Statement, fabricated by an identity thief and attached to an invalid income tax return is also invalid.
- (4) A Form W-2 filed by an employer that reports all the necessary information for the employee with a stolen SSN provided by the employee is a valid information return. The valid form reflects an employment relationship and is covered by IRC 6103(b)(1).

5.1.28.3.2  
(07-14-2021)  
**Tax Return Information - Refund Fraud**

- (1) Per IRC 6103(b)(2) - The term "return information" means a taxpayer's identity, the nature, source, or amount of income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense.
- (2) The information reported by an identity thief on a return is considered return information under IRC 6103(b)(2)(A).

5.1.28.3.3  
(07-14-2021)  
**Tax Return Information - Forms W-2 and 1099**

- (1) The return information on Form W-2, Wage and Tax Statement, and Form 1099, Miscellaneous Income, with a stolen SSN is the return information of both the employer who filed it and the employee/individual who used the SSN for employment.

- (2) Also, see IRM 11.3.2.4.1.2, Identity Theft and Access to Tax Returns and Information Returns, regarding disclosing information from Form W-2 and Form 1099.

5.1.28.3.4  
(07-14-2021)  
**Victim Disclosure**

- (1) Information used by the IRS to determine the victim's tax liability is return information and can be disclosed to the victim. This includes information related to the original assessment that was based on the Form 1040, Form W-2, or Form 1099 filed under the victim's SSN.

**Caution:** Do not disclose the identity or location of the identity thief to the taxpayer.

- (2) Information not used by the IRS to determine the victim's tax liability, including information about the IRS's investigation of the person who misuses the victim's SSN, is not the return information of the victim and may not be disclosed to the victim.
- (3) An identity-theft victim may obtain from the IRS a copy of the "bad return" and other return information associated with the processing of the "bad return" filed by the identity thief if the disclosure will not seriously impair federal tax administration. Information about the IRS's investigation is not the return information of the victim and may not be disclosed to the victim. Instructions for taxpayers to request a copy are available on IRS.gov, <https://www.irs.gov/Individuals/Instructions-for-Requesting-Copy-of-Fraudulent>Returns>.

5.1.28.3.5  
(05-15-2014)  
**Employer Disclosure**

- (1) An incorrect SSN on a Form W-2 is employer return information; however, any information about the investigation of the use/theft of the SSN or the person who used the SSN for employment cannot be disclosed to the employer.

5.1.28.4  
(03-24-2023)  
**Collection Activity in Identity Theft Cases**

- (1) When the taxpayer claims to be a victim of identity theft and the identity theft claim has **not** been received, do not release the levy unless one of the circumstances described in IRM 5.11.2.3.1, Legal Basis for Releasing Levies, exists.
- (2) When the taxpayer claims to be a victim of identity theft and an identity theft claim has been received, release any levy in effect only for the tax modules affected by the identity theft.
- (3) If there is a balance due not attributable to identity theft, then collection activities, including the appropriate use of enforced collection action, are not prohibited when a taxpayer has established that they were a victim of identity theft. However,
  - a. Be sensitive to the adverse impact that being a victim of identity theft may have upon a taxpayer and their ability to pay.
  - b. Consider temporarily suspending the account until the identity theft incident is resolved in cases where you determine the identity theft will have an adverse impact on the taxpayer's ability to pay.

**Caution:** Ensure collection activities are taken only on balance due modules not attributable to identity theft.

5.1.28.4.1  
(07-14-2021)  
**Assessment is Result of Identity Theft**

- (1) If the taxpayer is a victim of identity theft, review the case history for any outstanding enforcement activity that may need to be addressed, e.g., levies, liens, and bankruptcy claims.

- (2) Cases in inventory will not be systemically blocked from automated levy action, (e.g., State Income Tax Levy Program (SITLP), and Federal Payment Levy Program (FPLP)). Manually block the case from levy by requesting the appropriate IDRS input if the assessment is a result of identity theft.
- (3) See IRM 5.12.11.2.1, Identity Theft and Liens, for additional procedures regarding Notices of Federal Tax Lien (NFTL).
- (4) See IRM 5.9.5.12, Identity Theft (IDT) - Introduction, for additional procedures regarding taxpayers in bankruptcy.

5.1.28.4.1.1  
(04-26-2018)

#### Returning Levied Property in Cases of Identity Theft

- (1) See IRM 5.11.2.3.6, Levy Releases in Cases of Identity Theft, for guidance on returning levied property to **persons other than the taxpayer**. The levy of an asset belonging to someone other than the person against whom the tax was assessed is called a “wrongful levy”. The authority to return wrongful levy payments is provided in IRC 6343(b), which limits the return of money to the period of time within two (2) years from the date of the levy.

**Example:** Taxpayer has balance due. Another person is using the taxpayer’s SSN for employment and the other person’s wages are levied (levy date was after March 22, 2017). The levy payments may only be returned within two (2) years from the date of the levy.

- (2) The time frame for returning levied property to **the taxpayer** is the same as the time frame for returning wrongfully levied property. In this case, we have an assessment against the taxpayer and have levied against the taxpayer. Under our normal operating procedures, when we learn that the return that was filed was not the taxpayer’s return, we will remove (back out) the return and the erroneous refund that went to the thief. The taxpayer’s account will have a zero liability and a credit balance equal to the amount of levy proceeds. Because the assessment and levy were for the taxpayer/victim rather than an assessment for a taxpayer and a levy on a third-party, the two (2) year wrongful levy statute does not apply. However, because the assessment is invalid, the levy is considered to be erroneous and the levy proceeds may be returned to the victim under IRC 6343(d) if requested by the taxpayer within two years after the date of the levy. If you have cases where the taxpayer comes in more than two years after the payment, Counsel would need to consider whether there is another legal theory that would support returning the proceeds to the taxpayer/victim.

**Example:** An identity thief has filed a return in the taxpayer’s name and the taxpayer did not have a filing obligation. The taxpayer was unaware that they were a victim of identity theft. In the interim, the identity theft return either was audited or reviewed and there is an assessed balance on the victim’s account that IRS is attempting to collect (defaulted deficiency or summary assessment of overstated withholding). IRS uses its levy authority to collect against the assessment by levying the taxpayer. Sometime later the victim comes forward and informs IRS of the identity theft. The IRS applies the two-year period applicable to return of proceeds from erroneous levies.

5.1.28.4.1.2  
(03-24-2023)

## Returning Accounts to Currently not Collectible Status

- (1) Accounts previously reported currently not collectible (CNC), unable to pay, may be reactivated when the taxpayer is the victim of stolen identity refund fraud.

**Example:** Fraudulent refund from a 2021 return offsets to balance due for 2020 reported CNC. The total positive income (TPI) on the 2021 return is above the CNC closing code and the 2020 balance due is reactivated.

**Note:** The CNC should be re-activated, barring unresolved issues arising since the input of the original CNC closure.

- (2) See possible scenarios in the If/Then table below.

If	Then
the taxpayer is not required to file for 2021 or the TPI on the taxpayer's correct 2021 return is below the CNC closing code amount	return the 2020 module to CNC status without securing a new Collection Information Statement (CIS).
the TPI on the taxpayer's correct 2021 return is above the CNC closing code amount	secure a new CIS and make a new collectability determination.
the taxpayer owes on the correct 2021 return	secure a new CIS and include all balance dues in case resolution. <b>Exception:</b> A new CIS is not required if the conditions of IRM 5.16.1.3.3, Cases Reported Currently Not Collectible Based Upon a Prior Form 53, are met.
the taxpayer has not filed 2021 as required	secure return and follow guidance above as appropriate.

- (3) When the fraudulent refund offsets to the module in CNC, but does not full pay it and the TPI on the identity theft return is below the CNC closing code, the CNC module is not reactivated. If the TPI on the taxpayer's correct return is above the CNC closing code, the CNC module will be reactivated when the correct return is assessed.
- (4) For balance dues resulting from the reversal of a fraudulent refund that full paid an account in CNC, follow the procedures in this table:

If	Then
an NFTL was released	revoke the release and file a new NFTL after the erroneous refund is reversed.
the taxpayer does not have a filing requirement for subsequent tax years or the TPI on subsequent year's returns is below the CNC closing code	do not secure a new CIS and reinstate the module(s) to CNC status.
the TPI on the taxpayer's correct return is above the CNC closing code and/or the taxpayer owes on the correct return	secure a new CIS and include all balance dues in the case resolution. <b>Exception:</b> A new CIS is not required if the conditions of IRM 5.16.1.3.3, Cases Reported Currently Not Collectible Based Upon a Prior Form 53, are met.

- (5) For a balance due reversed out of CNC status when the taxpayer is a victim of employment related identity theft and the addition of the unreported income increases the TPI to greater than the CNC closing code, verify the taxpayer's income and if the taxpayer's income is,
- Less than the CNC closing code, then do not secure a new CIS and return the module to CNC status.
  - Greater than the CNC closing code, then secure a new CIS unless the CIS in the case file is less than 12 months old.

5.1.28.4.1.3  
(03-24-2023)

#### Returning Accounts to Installment Agreement Status

- (1) Work balance due accounts resulting from the reversal of fraudulent refunds that full paid accounts in installment agreement (IA) status 60 as described in the table below:

If	Then
the NFTL was released	revoke the release and file a new NFTL after the erroneous refund is reversed.
there is no balance due on the taxpayer's correct return	reinstate the IA and waive the user fee unless there are additional issues not related to the identity theft that arose after granting the original TC 971 AC 063 (ST. 60). A new Collection Information Statement (CIS) is not required.

If	Then
there is an unpaid balance due on the taxpayer's correct return	secure a new CIS and include all balance dues in the case resolution. <b>Exception:</b> A new CIS is not required if the CIS in the case file is less than 12 months old per IRM 5.15.1.2, Financial Analysis, Overview and Expectations.
the taxpayer is required to file a return that has not been filed	secure the return and follow guidance above as appropriate.

- (2) Balance due accounts could result from an additional assessment based on false withholding and/or credits on an identity theft return that causes the IA to default.

**Example:** A fraudulent refund from 2021 offsets to and partially pays a liability for 2020 in IA status. An additional assessment is subsequently made on 2021 for the false withholding that defaults the IA. Apply the procedures in the following table for this example in similar cases.

- (3) See possible scenarios in the If/Then table below:

If	Then
the taxpayer is not required to file for 2021 or there is no balance due on the 2021 return	reinstate the 2020 module to IA status and waive the user fee unless there are additional issues not related to the identity theft that arose after granting the original TC 971 AC 063 (ST. 60).
the taxpayer owes for 2021	secure a new CIS and include all balance dues in the case resolution. <b>Exception:</b> A new CIS is not required if the CIS in the case file is less than 12 months old per IRM 5.15.1.2, Financial Analysis, Overview and Expectations.
the taxpayer has not filed 2021 as required	secure the return and follow guidance above as appropriate.

- (4) Follow the procedures in the table below for balance due accounts resulting from an IA that defaulted because of an assessment based on income earned by someone other than the taxpayer that was reported under the taxpayer's SSN.

If	Then
all of the taxpayer's income was verified and reported with no balance due	reinstate the IA and waive the user fee unless there are additional issues not related to the identity theft that arose after granting the original TC 971 AC 063 (ST. 60).
all of the taxpayer's income is verified, but has not been reported resulting in an additional balance due	secure a new CIS and include all balance dues in the case resolution. <b>Exception:</b> A new CIS is not required if the CIS in the case file is less than 12 months old per IRM 5.15.1.2, Financial Analysis, Overview and Expectations.

5.1.28.5  
(03-24-2023)

#### Types of IMF Identity Theft

- (1) For IRS purposes, the two types of IMF identity theft are:

- non tax-related
- tax-related

- (2) In non-tax-related identity theft:

- A taxpayer's (or dependent's) wallet, driver's license, SSN, or credit card are lost or stolen. However, if there is no indication that the lost or stolen information is being used for tax purposes, then this is a case described as identity theft not related to tax administration.
- Individuals may self report an identity theft incident with no existing tax-related consequence by contacting the Identity Protection Specialized Unit (toll free 800-908-4490), and submitting an identity theft claim. The IRS will input an indicator (TC 971, AC 504) on their account, and future incidents related to tax administration will not require a claim to be submitted again.
- When any taxpayer (or dependent) needs assistance regarding non tax-related identity theft with no known tax administration impact, refer them to the Identity Protection Specialized Unit at 1-800-908-4490.

- (3) The two types of IMF identity theft related to tax administration are as follows:

- An identity thief has used a taxpayer's (or dependent's) SSN and other Personally Identifiable Information (PII) for employment purposes.

**Example:** A taxpayer may not be aware that someone in another state has used their SSN for the purposes of getting a job. When IRS records are matched against Social Security records, the IRS shows that the taxpayer has not reported that additional income earned by the identity thief on their tax return. The taxpayer may receive a notice or tax bill related to that additional unknown income or may even receive a notification of an audit to get the issue resolved. If the taxpayer is not required to file a tax return, there may be a Substitute for Return (SFR) assessment based on the income earned by the identity thief.

- b. An identity thief has used a taxpayer's (or dependent's) SSN and other PII for fraudulent filing purposes.

**Example:** A taxpayer may file their 2020 tax return on May 17, 2021. The IRS may reject the return because an unknown person has already filed a tax return under their SSN. The taxpayer will experience a delay in receiving their refund because the identity thief has already filed a fraudulent return and received a fraudulent refund using the unsuspecting taxpayer's SSN.

- c. Continue to work all tax-related identity theft issues in your inventory that have an impact on tax administration and do not refer such a case to the Identity Protection Specialized Unit.

**Note:** If you are contacted by a taxpayer (or dependent) who is a victim of identity theft, and there is no open case on the taxpayer, whether it is tax-related identity theft or non tax-related identity theft, refer the taxpayer to the Identity Protection Specialized Unit, 1-800-908-4490.

5.1.28.5.1  
(03-24-2023)  
**IMF Identity Theft  
(Revenue Protection)  
Return with Unpostable  
Code (UPC 126, MFT 32)**

- (1) The IRS established the Taxpayer Protection Program (TPP) to identify and prevent the processing of potentially fraudulent returns. The program was established to help combat identity theft by preventing fraudulent returns from being filed using another person's SSN. For these accounts, any Incoming tax returns using the taxpayer's SSN are to be systemically screened using a series of filters in an attempt to distinguish legitimate tax returns from fraudulent returns. If the tax return is deemed to be potentially fraudulent, processing of the tax return is halted and the return is sent to the unpostable unit. Refer to IRM 5.1.11.5.11, The Taxpayer Protection Program, to identify early detection of potentially fraudulent tax returns with indications of identity theft.
- (2) If the identity theft return is posted on MFT 32, then the revenue officer needs to determine whether there is apparent identity fraud connected with the return. The MFT 32 is subject to the revenue officer's verification and checks to verify the return filing legitimacy. See IRM 5.1.11.5.12, MFT 32 and Unpostable 126 procedures, to authenticate the taxpayer's identity. When a return is flagged, the system freezes the claimed tax refund until the return's legitimacy is verified.
- (3) If the flagged return is, in fact, legitimate, the return needs to be moved (reversed) from MFT 32 to MFT 30 for the refund to be issued.
- (4) If an unpostable condition appears on an account on IDRS, and there are indicators of an open TPP issue, the revenue officer must follow the procedures

outlined in IRM 25.25.6.2.3, Exam/Collection/Compliance Office Employees - Procedures for Cases with Taxpayer Protection Program (TPP) Involvement, to resolve the account.

5.1.28.6  
(03-24-2023)

**Standard IMF Tax  
Related Identity Theft  
Claim Requirements**

- (1) To reduce the burden on individual taxpayers, the IRS has established standard claim requirements for cases that involve identity theft.
- (2) See IRM 5.1.28.8.2, Step 2 below to determine if an identity theft claim is required. In addition, IRM 25.23.2.3, Identity Theft Claims - General Guidelines, provides the claim policy for all operating divisions and functions.
- (3) If required, request the Form 14039, Identity Theft Affidavit when a taxpayer alleges that they are a victim of identity theft.

**Note:** Form 14039 no longer requires the submission of additional information/documentation. Form 14039 will be used to obtain additional information from the taxpayer to support the identity theft claim only if internal/external resources available fail to authenticate the request of identity theft.

- (4) Establish a 30-day deadline for the taxpayer to submit a claim.

**Note:** If the taxpayer states they previously provided the claim, check Document Viewer on the Accounts Management System (AMS) to see if the documentation was scanned into Correspondence Imaging Inventory (CII).

- (5) Accept a claim from the taxpayer or someone who has power of attorney for the taxpayer pursuant to Form 2848, Power of Attorney and Declaration of Representative .

5.1.28.6.1  
(07-14-2021)

**When to Request  
Additional Information to  
Support Claim/Allegation  
of Identity Theft**

- (1) If unable to resolve the account by using internal information sources and/or by information already provided by the taxpayer, request additional information. Refer to IRM 25.23.2.3.6, When to Request Additional Information to Support an Allegation of Identity Theft. Taxpayer information to substantiate identity theft may include:

- a. Authentication of Identity - A copy of a valid U.S. federal or state government-issued form of identification to authenticate identity.

**Example:** Driver's License, State Identification Card, Social Security Card, Passport, etc.

**Note:** This link provides a list of acceptable primary and secondary forms of identification: <https://www.fedidcard.gov/document/acceptable-forms-id?download=1&?download=109>.

- b. Evidence of identity theft - Police Report, or Form 14039, Identity Theft Affidavit.

**Note:** Form 14039 should only be requested when the taxpayer has not previously submitted the form or when the submitted form was illegible.

- c. Payor documents - such as W-2 or 1099, utility bills, deeds, or other proof of residency.

5.1.28.6.2  
(07-14-2021)  
**Acknowledging and  
Handling IMF Identity  
Theft Claim**

- (1) Follow the information in this table regarding acknowledging receipt of the taxpayer's claim/additional information:

If	Then
the identity theft claim is received in person	no additional acknowledgement of receipt is needed.
the identity theft claim is not received in person	acknowledge receipt within 30 days.
receipt acknowledgement is sent in the mail	be sure it is sent to the right address. <b>Caution:</b> The address on the Form 14039, Identity Theft Affidavit, may be different from the case address.

- (2) A claim should be legible and accurately associated with the correct taxpayer.
- (3) Apply stringent safeguards when storing and retaining a claim. Store the claim along with the case file.
- (4) Secure and handle a claim and information in the same manner as other sensitive taxpayer personal information.
- (5) See IRM 5.1.28.8.2, Step 1 below for procedures to request input of TC 971, AC 522 PNDCLM. If after the account has been marked with identity theft indicator, the employee determines identity theft did not occur or the taxpayer did not provide supporting documents (Form 14039 or police report and personal identification), the identity theft tracking will be reversed. This removes the case from identity theft inventory. See IRM 5.1.28.8.6, Identity Theft Code TC 971 AC 522 Reversal Procedures (TC 972 AC 522), for additional guidance.
- (6) After receipt of the taxpayer's identity theft claim, conduct research to verify the taxpayer's claim.
- (7) If the identity theft claim received is not complete or legible, but a determination can be made based on internal research, then proceed using the internal research results.

5.1.28.7  
(06-20-2017)  
**Making an Identity Theft  
Determination**

- (1) Employees assigned an identity theft case will treat the identity theft victim's account as a whole, resolving all account issues.
- (2) Perform research to determine the effect of the identity theft on all tax years. At a minimum, if applicable, review the three prior years and all subsequent tax years when analyzing the taxpayer's account.
- (3) Rule out the following:
- a. A mixed entity that occurs when two or more returns post for the same period using the same TIN due to an error by the taxpayer, return preparer, or IRS.

- b. A scrambled SSN when the Social Security Administration assigns the same SSN to more than one taxpayer.
- (4) Do not assume that the taxpayer filing the identity theft claim is the true owner of the SSN. Review the case and consider all information received and available through research to determine the legitimate taxpayer.
- (5) Use all available research tools to determine the validity of the identity theft claim. Keep in mind that identity theft for employment purposes and identity theft for fraudulent filing purposes will require different research.

5.1.28.7.1  
(07-14-2021)

**Validating Claim of  
Identity Theft for  
Fraudulent Filing  
Purposes**

- (1) The following is a list of the common research tools available to validate the claim. This list is not all inclusive:
  - a. IDRS for prior and subsequent years for filing status, address, dependents claimed, and Schedules A/B/C/D/E/F information for comparison to the TC 150 return and any subsequent returns submitted.
  - b. CC IRPTR for payer documents that may verify income, deductions, and address information reported.
  - c. CC TRDBV for bank routing and preparer information that may be useful.
  - d. CC IMFOLE, CC INOLES, and CC RTVUE are other research command codes available.
  - e. Available locator sources.
- (2) If additional clarification or information is needed, contact the taxpayer and request the information.

5.1.28.7.2  
(07-14-2021)

**Validating Claim of  
Identity Theft for  
Employment Purposes**

- (1) The following is a list of suggested documents that can be secured from the employer that may help to verify a taxpayer's claim of employment-related identity theft. The list is not all inclusive and not all documents will be necessary in every circumstance:
  - a. Application for employment
  - b. Form I-9 (IMMIGRATION), Employment Eligibility Verification
  - c. Form W-4, Employer's Withholding Allowance Certificate
  - d. Internal documents such as insurance forms
  - e. Copies of cancelled pay checks with endorsement
  - f. Copy of work photo badge or other employment photos
  - g. Copy of the driver's license and Social Security card provided to gain employment
  - h. Copy of work history with dates missed, location of actual work

**Caution:** Before making a third-party contact, the IRS must confirm that applicable requirements of IRC 7602(c) are satisfied or the taxpayer has given consent to such third party contact. Refer to IRM 25.27.1, Third-Party Contact Program, for general servicewide guidance and IRM 5.1.1.12, Third Party Contacts, for servicewide guidance in collection casework.

- (2) Consider the following when reviewing the documentation:
  - a. Is the taxpayer's address different from the unreported income employer's records?
  - b. Is the handwriting on the documents collected from the taxpayer and the unreported income employer's records distinctly different?

- c. What is the distance from the taxpayer to employment location for the unreported income?
- d. Could the taxpayer have worked for both employers on the same dates?
- e. Do the photo identifications from the unreported income employer match that of the taxpayer?

(3) Research available locator sources.

(4) If additional clarification or information is needed, contact the taxpayer and request the information.

5.1.28.8  
(03-24-2023)  
**Identity Theft Case Resolution**

- (1) Resolve the case in an appropriate manner according to the following procedures depending on whether the:
  - a. Taxpayer establishes that they are a victim of identity theft
  - b. IRS employee determines identity theft occurred
  - c. Taxpayer does not establish that they are a victim of identity theft or
  - d. Taxpayer committed identity theft.
- (2) **No matter how the case is resolved, if initial identity theft indicators are on the account (TC 971 AC 522), closing identity theft indicators (TC 971 AC 501/506 or TC 972 AC 522) must be requested.**

5.1.28.8.1  
(07-14-2021)  
**Individual Taxpayer Alleged Identity Theft vs. IRS Identified Identity Theft**

- (1) Identity theft can be alleged by the taxpayer or identified by an IRS employee.
- (2) If an identity theft claim is secured from the taxpayer, follow IRM 5.1.28.8.2, Individual Taxpayer Alleges Identity Theft, for inputting the appropriate TC 971 action codes.
- (3) If an identity theft claim is not secured from the taxpayer, follow IRM 5.1.28.8.3, IRS Identified Identity Theft, for inputting the appropriate TC 971 action codes.

5.1.28.8.2  
(03-24-2023)  
**Individual Taxpayer Alleges Identity Theft**

- (1) Instances of identity theft can either be alleged by the taxpayer, or third-party such as a taxpayer representative or bankruptcy trustee.
- (2) Below are step-by-step instructions for inputting the identity theft transaction codes to identify the claim and source code and preparing Form 4844, Terminal Input Request, in instances of IMF taxpayer alleged identity theft.
- (3) Below are step-by-step instructions for inputting the identity theft transaction codes and preparing Form 3870, Request for Adjustment, in instances of IMF taxpayer alleged identity theft.

**Note:** For instructions in bankruptcy cases, see IRM 5.9.5, Opening a Bankruptcy Case.

Step	TC 971 Action Code	Employee Actions	Notes
1	TC 971 AC 522 <b>PNDCLM</b>	Request input of TC 971 AC 522 with source code <b>PNDCLM</b> using Form 4844 if the taxpayer alleges they did not earn income or did not file the return and has not yet provided an identity theft claim and a <b>PNDCLM</b> is not already present on CC ENMOD.	The Secondary Date field will reflect each tax year affected by identity theft. Use Form 4844, Terminal Input Request, to request input of the TC 971 AC 522 <b>PNDCLM</b> (see example at Exhibit 5.1.28-1). Forward to Designated Identity Theft Adjustment (DITA). See IRM 5.1.28.8.4(2)c, Form 3870 Preparation and Routing, for DITA contact information.
2	Table cell intentionally left blank.	<p>Review CC ENMOD to determine if the following conditions exist:</p> <ol style="list-style-type: none"> <li>1. There is a posted/unreversed TC 971 AC 501/ 506 or TC 971 AC 522 Source Code INCOME, MULTFL, INCMUL, NOFR, or OTHER <b>and</b></li> <li>2. The posted transaction falls within a minimum of three prior years <b>and</b></li> <li>3. The allegation relates to a previously reported incident.</li> </ol> <p>If above criteria is met, skip step 3. A claim is not required. If above criteria is not met, give the taxpayer a 30-day deadline to provide a claim.</p>	If the taxpayer states they previously provided the claim, review Accounts Management System (AMS) history and check to see if the request was attached or scanned into the Correspondence Imaging Inventory (CII).

Step	TC 971 Action Code	Employee Actions	Notes
3	TC 971 AC 522 with source code <ul style="list-style-type: none"> <li>• <b>INCOME</b> - income reported under taxpayer's SSN without their consent or knowledge</li> <li>• <b>MULTFL</b> - two or more returns filed under the same SSN for the same tax period</li> <li>• <b>INCMUL</b> - both INCOME and MULTFL apply</li> <li>• <b>NOFR</b> - taxpayer not required to file</li> <li>• <b>OTHER</b> - no other source code fits</li> <li>• <b>UNWORK</b> - identity theft claim received but has not been resolved yet.</li> </ul>	Request input of TC 971 AC 522 with appropriate source code when a complete and legible claim is received from taxpayer.	If the taxpayer does not provide a claim when requested and the 30-day deadline has expired, then reverse the TC 971 AC 522 with TC 972 AC 522 source code <b>NORPLY</b> . Use Form 4844 to request input and forward to DITA per contact information at IRM 5.1.28.8.4(2)c, Form 3870 Preparation and Routing. Continue with collection action following regular collection procedures after confirming all applicable appeal rights have been granted.
4	Table cell intentionally left blank.	Conduct research to determine if identity theft occurred. See IRM 5.1.28.7.1 for fraudulent filing and IRM 5.1.28.7.2 for employment related identity theft claims. For example, check Accurint, IRPTR, etc. If a paper tax return was filed, compare the signature on tax return to the signature on Form 14039. To obtain a copy of the paper refund check, see <a href="https://portal.ds.irsnet.gov/sites/VL131/Lists/ATAT/DispItemForm.aspx?ID=26&amp;Source=https%3A%2F%2Fportal%2Eds%2Eirsnet%2Egov%2Fsites%2FVL131%2FLists%2FAtat%2FAAllItems%2Easpx&amp;ContentTypeId=0x0100124E5409CBF2EB4FBBE160EEE84DFC40">https://portal.ds.irsnet.gov/sites/VL131/Lists/ATAT/DispItemForm.aspx?ID=26&amp;Source=https%3A%2F%2Fportal%2Eds%2Eirsnet%2Egov%2Fsites%2FVL131%2FLists%2FAtat%2FAAllItems%2Easpx&amp;ContentTypeId=0x0100124E5409CBF2EB4FBBE160EEE84DFC40</a> .	If after review it is determined that identity theft did not occur, reverse the TC 971 AC 522 with TC 972 AC 522 source code <b>NOIDT</b> . Use Form 4844 to request input and forward to DITA per contact information at IRM 5.1.28.8.4(2)c. See example of Form 4844 at Exhibit 5.1.28-2.

Step	TC 971 Action Code	Employee Actions	Notes
5	Table cell intentionally left blank.	Ensure taxpayer's address is updated to correct address. See IRM 25.23.2.3.7, When to Update the Victim's Address.	Table cell intentionally left blank.
6	TC 971 AC 501	Prepare Form 3870 to correct taxpayer's account. Notate on Form 3870 to input TC 971 AC 501.	TC 971 AC 501 is input when account has been corrected.
7	TC 470 CC 90	Request input of TC 470 CC 90 if the module will be fully abated creating no remaining balance due.	Table cell intentionally left blank.
8	Table cell intentionally left blank.	If the taxpayer's case is fully resolved and no issues remain, send Letter 4222, Field Collection Case Resolution, to victim prior to closing case on ICS.	Table cell intentionally left blank.

- (4) Routing information for Form 3870 in IMF identity theft cases can be found at IRM 5.1.28.8.4(2)b. The routing will depend on the type of assessment that is being adjusted.

5.1.28.8.3  
(03-24-2023)  
**IRS Identified Identity Theft**

- (1) During the normal course of business, you may determine that identity theft occurred and the case is not yet resolved. In most instances, you will attempt to secure the identity theft claim from the taxpayer.
- (2) If you are unable to secure the identity theft claim (for example, the taxpayer is deceased), or the taxpayer is unwilling to provide the identity theft claim because they are receiving the benefit of the refund from the identity theft return, follow the procedures for IRS identified identity theft.

**Example:** The refund due to the identity theft return was issued to the bankruptcy trustee. The trustee negotiated the check and applied it to debts of the taxpayer. Because the taxpayer received the benefit of a debt reduction due to the issuance of the refund on the identity theft return, the taxpayer may not want to provide the identity theft claim.

Step	TC 971 Action Code	Employee Actions	Notes
1	TC 971 AC 522 <b>IRSID</b>	Request input of TC 971 AC 522 with source code <b>IRSID</b> using Form 4844 if an IRS employee determines identity theft occurred.  <b>Exception:</b> TC 971 AC 522 <b>IRSID</b> is not used when an individual with an Individual Taxpayer Identification Number (ITIN) reports misusing an SSN belonging to someone else.	The Secondary Date field will reflect each tax year affected by identity theft. Use Form 4844 to request input of the TC 971 AC 522 with source code <b>IRSID</b> and forward to DITA per contact information at IRM 5.1.28.8.4(2)c for input.
2	Table cell intentionally left blank.	Ensure taxpayer's address is updated to correct address. See IRM 25.23.2.3.7, When to Update the Victim's Address.	Table cell intentionally left blank.
3	TC 971 AC 506	Prepare Form 3870 to correct taxpayer's account. Notate on Form 3870 to input TC 971 AC 506.	TC 971 AC 506 is input when account has been corrected.
4	TC 470 CC 90	Request input of TC 470 CC 90 if the module will be fully abated creating no remaining balance due.	Table cell intentionally left blank.
5	Table cell intentionally left blank.	If the taxpayer's case is fully resolved and no issues remain, send Letter 4222, Field Collection Case Resolution, to victim prior to closing case on ICS.	Table cell intentionally left blank.

- (3) The function that completes the account adjustment and inputs the TC 971 AC 506 requested on Form 3870 will notify the taxpayer (victim), by letter, that someone may have attempted to use their SSN. This victim notification letter will include information about:

- Identity theft prevention
- Identity theft related resources
- The identity theft indicator placed on their account

5.1.28.8.4  
(03-24-2023)  
**Form 3870 Preparation  
and Routing of IMF  
Tax-Related Identity  
Theft**

- (1) If it is determined that the individual taxpayer is a victim of identity theft, Form 3870, Request for Adjustment, is prepared to correct the victim's account. The following guidelines should be followed when preparing Form 3870:

- a. Enter "Identity Theft" in Item 11, Reason for Adjustment.
- b. A nullity or fraudulent filing is a return that was not filed by the SSN owner. If the assessment is based on a fraudulent return, notate on the Form 3870 that it should be treated as a nullity. For more information on nullity returns see IRM 25.23.4.8.1, Streamline Identity Theft (IDT) Case Identification and Processing.

**Note:** Form 1040 returns with Schedule C income see IRM 25.23.4.8.1.3, Identity Theft (IDT) with IRP Data, Refund Scheme or Schedule C Involvement.

- c. Include specific instructions on actions needed to correct the account. For example, state that TC 150 in amount of \$XX is the return filed by the identity thief. Indicate if there are any estimated tax payments that were made by the victim-taxpayer that should remain on the account or if a refund generated by the identity theft return was offset to another tax liability.
- d. If the taxpayer has been assessed a frivolous return penalty under IRC 6702 based on the return filed under the taxpayer's SSN by an identity thief, notate on Form 3870 to abate the frivolous return penalty. The penalty can be identified by MFT 55 with penalty reference code 543. The tax period must be the same as the identity theft return. The penalty must be abated by the Frivolous Return Program (FRP). See (4) below.
- e. Indicate on Form 3870 if contact is needed when the adjustment is completed.

**Example:** There is a balance due on the correct return secured from the taxpayer-victim and you will continue with collection actions after assessment. The function completing the adjustment will alert you when the adjustment is completed. A confirmation of account corrections will be sent via email. If email confirmation cannot be completed due to an incorrect or missing email address, Form 3870 will be mailed back to the originator as confirmation.

- f. Attach a copy of identity theft claim Form 14039, Identity Theft Affidavit (keep copies in the case file) to Form 3870.
- g. Attach an original return, if secured, from the victim-taxpayer (keep a copy in the case file) to Form 3870.
- h. -NUMIDENT - (optional) CC MFTRAU

**Exception:** If the spouse is the identity theft victim, then process the joint return on Form 795/795A to Submission Processing.

- i. Do not attach other IDRS prints.
- j. Request input of TC 971 AC 501 or AC 506 on Form 3870. The TC 971 will be input when the account is corrected.
- k. Forward Form 3870 to the appropriate function for adjustment based on type of assessment. See (2) below.
- l. Incomplete referrals will be rejected.
- m. To expedite Form 3870 notate "Expedite" at the top of the form per IRM 25.23.10.7.5, Post Function DITA Procedures.

- (2) The completed Form 3870 will be routed based on the type of assessment that needs to be adjusted.

- a. Examination, Automated Under Reporter (AUR), Substitute for Return (SFR)/Automated Substitute for Return (ASFR) assessments - for reconsideration prepare manual Form 3870 (Other template in ICS) and route to:

Kansas City Service Center IDTVA

333 W. Pershing Road

Kansas City, MO. 64108

MS 5050 P4

Fax number 855-663-7048

*mailto:\*W&I IDT:KC:SPEC-ACSS*

- b. Identity theft return – a return filed under the taxpayer's social security number by an identity thief. Prepare manual Form 3870 (OTHER template in ICS) and forward to DITA per contact information at IRM 5.1.28. 8.4(2)c below if there is not a subsequent Audit or AUR assessment. If an original return is attached to the Form 3870, then it must be mailed to DITA rather than faxed or sent electronically.

**Exception:** For non-masterfile cases, forward the Form 3870 to the Accounts Management NMF team at:

Philadelphia Campus, PAMC

2970 Market St., Mail Stop BLN 3-J23, Team 408

Philadelphia, PA 19104

- c. The contact information for the Designated Identity Theft Adjustment (DITA) team is as follows:

Email Address	Efax Number	Mailing Address
<i>mailto:*SBSE CCS DITA</i>	1-855-786-6575	Internal Revenue Service DITA Mail Stop 4-J30- 151 2970 Market St., Philadelphia, PA 19104

- (3) In cases involving employment related identity theft, also prepare Form 9409, IRS/SSA Wages Worksheet, to correct taxpayer wage records. Form 9409 includes the Social Security mailing address for the form.

- (4) If the taxpayer has been assessed a frivolous return penalty under IRC 6702 based on the return filed under the taxpayer's SSN by an identity thief, the civil penalty must be abated by the Frivolous Return Program (FRP). The penalty can be identified by MFT 55 with penalty reference code 543. The tax period must be the same as the identity theft return. A copy of the Form 3870 that was prepared and sent based on the routing instructions in (2) above should be sent to the FRP at the following address:

Ogden Compliance Services

Attn: FRP, M/S 4450

1973 N Rulon White Blvd

Ogden, UT 84404

5.1.28.8.5  
(05-15-2014)  
**IMF Identity Theft  
Indicator Codes**

- (1) The Identity Protection Program developed and implemented identity theft indicator codes to centrally mark and track identity theft incidents. Each indicator is input as a Transaction Code (TC) with Action Code (AC) and displayed on Integrated Data Retrieval System (IDRS) command codes ENMOD and IMFOL with the definer "E" on the affected taxpayer's account.
- (2) Request input or reversal of the identity theft transaction code according to the following procedures:
- When the identity theft victim is the secondary SSN on a joint account, the identity theft indicator is input on the secondary SSN. Identity theft indicators are not input on the primary SSN in these instances.
  - If both the primary and secondary taxpayers are victims, place the indicators on both SSN's.

5.1.28.8.5.1  
(07-14-2021)  
**Identity Theft Action  
Code Input Procedures**

- (1) Review CC ENMOD or CC IMFOLE for identity theft action codes.
- (2) If a previous identity theft incident was substantiated, the taxpayer does not need to send in a claim in order to re-substantiate. See IRM 25.23.2.3.6, When to Request Additional Information to Support an Allegation of Identity Theft.
- (3) Use Form 4844, Request for Terminal Action, to request input of the identity theft action code.
- (4) Forward completed Form 4844 to the Designated Identity Theft Adjustment (DITA) for input. See IRM 5.1.28.8.4(2)c for DITA contact information.
- (5) The IMF identity theft indicators are input on entity (CC ENMOD).

5.1.28.8.5.2  
(05-15-2014)  
**Completion of Form  
4844**

- (1) The IMF identity theft action code is input on the entity instead of being input to the applicable modules, so ensure that you follow these procedures to accurately complete Form 4844.
- (2) Complete the applicable blocks of Form 4844 including the following:
- "SSN"

- b. "Name control"
- c. "MFT code"

**Note:** Put "00" in "MFT" to indicate the entity.

- d. "Periods."

**Note:** Put "0000" in "Periods" to indicate the entity.

- e. "Name of taxpayer"
- f. "Remarks"

- (3) See IRM 5.1.28.8.5.3, Miscellaneous Fields, for instructions to complete the miscellaneous fields on the form and IRM 5.1.28.8.5.5, Remarks Block, for completing the "Remarks" block.
- (4) See IRM 5.1.28.8.5.4, Secondary Date Field, for instructions for entering the tax period ending date(s) in the Secondary Date (SECONDARY-DT) field.

## 5.1.28.8.5.3 (07-14-2021) Miscellaneous Fields

- (1) The miscellaneous field has three parts:
  - BOD / Function (Business Operating Division / Function)
  - Program Name
  - Tax Administration Source (Tax Admin Source)
- (2) Request input of the required miscellaneous field information in the "Miscellaneous Field Input" block of Form 4844.
- (3) Use the following codes to complete the first two miscellaneous fields:
  - a. BOD = "SBSE"
  - b. Program Name = as applicable, enter "CFBALDUE" or "CFDELRET"

**Note:** Use "CFBALDUE" for a combination balance due/delinquent return case.
- (4) Use the codes displayed in the following table to complete the third miscellaneous field (TC 971 AC 522 Tax Admin Source Codes):

Code	Usage
PNDCLM	The taxpayer makes an allegation of identity theft. The taxpayer has not yet provided the identity theft claim as required by IRM 25.23.2.3, Identity Theft Claims - General Guidelines.
UNWORK	Taxpayer identity theft claim received but has not been resolved yet.
IRSID	During the normal course of business, the IRS suspects identity theft occurred and the case is not yet resolved.
INCOME	Acceptable identity theft claim received from the taxpayer. Identity theft due to income reported under the taxpayer's SSN without their consent or knowledge.

Code	Usage
MULTFL	Acceptable identity theft claim received from the taxpayer. Identity theft due to two or more tax returns filed for the same tax period under the same SSN.
INCMUL	Acceptable identity theft claim received from the taxpayer. Identity theft due to both incomes reported under the taxpayer's SSN without their consent or knowledge and multiple filings (INCOME and MULTFL apply).
NOFR	Acceptable identity theft claim received from the taxpayer. Identity theft due to the victim (rightful taxpayer) not having a filing requirement.
OTHER	Acceptable identity theft claim received from the taxpayer. Identity theft which cannot be identified as related to any existing Tax Administration Source types.

- (5) No claim is required from the taxpayer if the taxpayer alleges identity theft and the following conditions exist:
- There is a posted unreversed TC 971 AC 501/506 or TC 971 AC 522 with Source Code INCOME, MULTFL, INCMUL, NOFR, or OTHER, and
  - The posted transaction falls within a minimum of three prior years as described in IRM 25.23.10.7.2.3, Processing Identity Theft Correspondence, and
  - The allegation relates to a previously reported incident as described in IRM 25.23.2.3.6, When to Request Additional Information to Support an Allegation of Identity Theft.
- (6) If the taxpayer asserts identity theft and provides a claim at the same time, mark the account with only TC 971 AC 522 with the appropriate Tax Administration Source Code.
- (7) Enter these codes into the miscellaneous field separated by a space.

**Example:** When receiving a claim for an identity theft incident that has an income related tax administration impact for SB/SE Field Collection (FC) on a delinquent return case, enter the following in the miscellaneous field:

<b>Miscellaneous Field Input</b>
<b>SBSE CFDELRET INCOME</b>

5.1.28.8.5.4  
(03-24-2023)

#### Secondary Date Field

- (1) Request input of the secondary date field information in the "Secondary Date Field" block of Form 4844.

- (2) The secondary date (SECONDARY-DT>) will contain the tax year(s) that are affected by the identity theft. Use MMDDYYYY format of the tax year affected by the identity theft incident.

**Example:** If a taxpayer substantiates identity theft and the impacted tax year is TY 2020, the SECONDARY-DT field input would be:

Secondary Date Field Input
12312020

**Example:** If a taxpayer substantiates identity theft and the impacted tax years are TY 2020 and TY 2021, the SECONDARY-DT field input would be:

Secondary Date Field Input
12312020

Secondary Date Field Input
12312021

- (3) Complete Form 4844, Request for Terminal Action, to request input of the identity theft action code and forward to DITA within 48 hours.

## 5.1.28.8.5.5 (05-15-2014) Remarks Block

- (1) Include the following in “Remarks” of Form 4844, “Input TC 971 AC XXX under ENMOD.”
- (2) Enter any other key pertinent information about the case in the “Remarks” block.

**Example:** “received valid Driver’s License and affidavit”

## 5.1.28.8.6 (07-14-2021) Identity Theft Code TC 971 AC 522 Reversal Procedures (TC 972 AC 522)

- (1) TC 972 AC 522 is used to close identity theft allegations when the IRS determines that identity theft has not occurred or in situations where the taxpayer fails to provide an identity theft claim as described in IRM 5.1.28.6(2).
- (2) For effective identity theft case tracking and reporting, include the Administration Source Fields on Form 4844 when appropriate depending upon the facts and circumstances of the case. The following table provides the Source Codes, their descriptions and Secondary Date Fields needed for IDRS input of TC 972 AC 522.

Term/Acronym	Description: Administration Source Code	Secondary Date Field
Identity theft has NOT occurred ( <b>NOIDT</b> )	In the course of resolving an identity theft issue, the employee assigned determines no identity theft occurred.	Will match the tax year of the TC 971 522 PNDCLM or TC 971 AC 522 IRSID as applicable.
The taxpayer did not provide supporting documents ( <b>NORPLY</b> )	This code is used to close identity theft claim when the taxpayer fails to provide the requested identity theft claim within the time specified by the employee assigned.	Will match the tax year of the TC 971 522 PNDCLM.

5.1.28.8.7  
(03-24-2023)  
**Identity Theft Code TC  
971 AC 501 and AC 506  
Reversal Procedures**

- (1) In some instances it may be necessary to reverse a TC 971 AC 501 or TC 971 AC 506 identity theft action code. Reversal may be necessary because of any of the following reasons:
  - a. The taxpayer requests reversal.
  - b. There was a keying or internal error in the input of the action code.
  - c. The original identity theft claim was fraudulent.
  - d. The action code has an internally identified negative affect on the taxpayer.
  - e. There are other reasonable circumstances not listed above.
- (2) Use Form 4844, Request for Terminal Action, to request the input of TC 972 with the action code 501 or 506.
- (3) Complete the miscellaneous fields with any applicable, specific information for detailed reporting. The miscellaneous field has three parts:
  - BOD / Function (business operating division / function)
  - Program Name
  - Reason
- (4) Request input of the required miscellaneous field information in the Miscellaneous Field Input block of Form 4844.
- (5) Use the following codes to complete the first two miscellaneous fields:
  - a. BOD = "SBSE"
  - b. Program Name = as applicable, enter "CFBALDUE" or "CFDELRET"

**Note:** Insert "CFBALDUE" if you have a combination balance due/delinquent return case.

- (6) Use the codes displayed in the following table to complete the third miscellaneous field (reason field codes and descriptions):

Reason Field Code	Description
TPRQ	Taxpayer Request: The taxpayer requests the 971 to be reversed. The taxpayer may feel that the issue has been resolved or it is no longer needed and is impacting them negatively.
IRSERR	Keying Error or Other Internal Mistake: The 971 was due to a typographical mistake or another internal mistake and should be reversed.
IRSADM	Internally Identified Negative Impact: The 971 is causing a negative impact on another internal process or system, and should be reversed to discontinue any negative impact.
FALSE	Fraudulent identity theft claim: The original identity theft incident claim was determined to be fraudulent.
OTHER	If codes (1)-(4) above are not applicable, use OTHER.

- (7) Complete the miscellaneous fields for TC 972 in the same format as for TC 971.

5.1.28.8.7.1  
(05-15-2014)

## Secondary Date Field — TC 972

- (1) The 972 will also use the SECONDARY-DT field to indicate which 971 will be reversed. When the 972 is applied, enter the tax year in the SECONDARY-DT field to designate the 971 that should be reversed.
- (2) Use MMDDYYYY format of the tax year affected by the identity theft incident.

5.1.28.9  
(03-24-2023)

## Taxpayer is Not a Victim of Identity Theft

- (1) Do not manually block the case from levy if the assessment is not a result of identity theft.
- (2) Follow normal collection procedures if the taxpayer does not establish they were a victim of identity theft.
- (3) If a TC 971 transaction code was input, then request reversal using TC 972.
- (4) Advise the taxpayer that the identity theft claim has not been substantiated.
- (5) If the taxpayer requests to have their case reviewed by a supervisor, give the taxpayer the name, telephone number, and address of your group manager.

5.1.28.10  
(06-20-2017)

**Taxpayer Committed  
Identity Theft for  
Purposes of Tax Evasion**

- (1) When indicators (badges) of fraud are uncovered, document the potential fraud indicators and initiate a discussion with your group manager. See IRM 25.1.2.3, Indicators of Fraud, to help you recognize the signs of fraud.

**Note:** An identity theft case referred to Criminal Investigation (CI) must have a tax or money laundering fraud/violation associated with it. Identity theft violations are not intended to be a stand alone violation. See IRM 9.5.5.2.4, Title 18 USC 1028 and 18 USC 1028A, Identity Theft.

- (2) If your manager concurs there are indicators of fraud warranting fraud development, contact the local fraud technical advisor (FTA) to determine if the case should be developed further as a potential fraud case, see IRM 25.1.2.2, Fraud Development Procedures.
- (3) A plan of action should be mutually developed between you, the FTA and the group manager to address the indicators of fraud present, see IRM 25.1.2.3(6), Indicators of Fraud - Conduct of Taxpayer.
- (4) Once firm indicators of fraud have been established and the case meets criminal criteria, refer the case to CI, see IRM 25.1.8.10, Collection Case Disposition.
- (5) If it is determined not to pursue a fraud referral, then correct the account as appropriate and follow normal collection procedures.

5.1.28.11  
(03-24-2023)

**Compliance Against  
Persons Using Another  
Person's SSN for  
Employment**

- (1) If someone using another person's SSN for employment has unfiled returns and it does not rise to level of tax fraud, consider making an enforcement referral. See IRM 5.1.11.7.3, Enforcement Referrals - Individual Master File (IMF) Del Ret. If the taxpayer does not have an Individual Taxpayer Identification Number (ITIN), request an IRS Number (IRSN) using Form 9956, Request for Temporary IRSN.
- (2) Consider making a referral to the Social Security Administration through Disclosure for the non-tax crime of misuse of an SSN. Disclosure to other federal agencies is permissible under IRC 6103(i)(3)(A). Only information that comes from a third-party source will qualify as information that can be released under this statute. Contact the employers on IRP documents to secure employment related documents such as copies of Social Security cards, state photo identification, and Form W-9, Request for Taxpayer Identification Number and

Disclosures of Return Information (Other than Taxpayer Return Information) Concerning Non-Tax Criminal Violations, for more information on these referrals.

**Caution:** Before making a third-party contact, the IRS must confirm that applicable requirements of IRC 7602(c) are satisfied or the taxpayer has given consent to such third party contact. Refer to IRM 25.27.1, Third-Party Contact Program, for general servicewide guidance and IRM 5.1.1.12, Third Party Contacts, for servicewide guidance in collection casework.

- (3) A taxpayer not eligible for an SSN must use an individual taxpayer identification number (ITIN) when filing their return.

#  
#

- (4) An employer cannot use an ITIN on a Form W-2, but must instead use the SSN that the taxpayer provided in order to obtain employment. A Form W-2 filed by an employer that reports all the necessary information for the employee with a stolen SSN that was provided by the employee is considered a valid information return. The fact that a Form W-2 contained the SSN of someone other than the employee is the return information of the employer and that fact alone may be disclosed to the employer.

**Note:** This type of case should not be sent to either IDTV or Fraud as the Internal Revenue Code recognizes these as legal returns.

- (5) Once ITIN information is verified and it does not rise to the level of fraud, proceed with normal collection procedures.

5.1.28.12  
(03-24-2023)

## Erroneous Identity Theft Refund Issued to Victim

- (1) There are several situations in which the taxpayer/victim, through no fault of their own, may receive the benefit of the refund from the return filed by the identity thief.

**Example:** The identity thief filed a return under the taxpayer-victim's SSN and the refund is offset to the taxpayer-victim's child support obligation, student loan, or other type of Treasury Offset Program offset.

**Example:** In a bankruptcy case with a refund turnover order, the trustee received the refund check. It has already been applied to the debtor's bankruptcy case and disbursed to creditors in the bankruptcy plan. The check is not available to return.

- (2) See IRM 21.4.5.12, How to Repay an Erroneous Refund or Return an Erroneous Refund Check or Direct Deposit, on returning erroneous refunds.
- (3) If the taxpayer does not voluntarily return the refund, there are two remedies to recover the refund from the taxpayer/victim:
  - a. Erroneous refund suit as authorized by IRC 7405. See IRM 5.17.4.14, Suits to Recover Erroneous Refunds.
  - b. Common law right of offset (Category D erroneous refund) – within two years from the date that refund was sent out
  - c. See IRM 21.4.6, Refund Offsets Procedures.

**Note:** Any refunds offset through the Treasury Offset Program (TOP) will be recovered through the TOP reversal process so no other remedies need be pursued.

5.1.28.13  
(03-24-2023)

## BMF Identity Theft

- (1) BMF identity theft is defined by the filing of a business tax return when someone creates, uses, or attempts to use a business's or individual's identifying information without authority to obtain tax benefits, or to enable fraudulent schemes. See also IRM 25.23.9, Business Master File (BMF) Identity Theft Processing, for general guidance for all employees working cases involving BMF identity theft.
- (2) In the course of an investigation, the taxpayer may allege they are the victim of identity theft or other factors may point to BMF identity theft, such as:
  - a. Fictitious business

- b. Business inactive during the period in question
  - c. A third-party established and operated the business using another individual's identifying information
- (3) The taxpayer may not have been aware of the theft until contacted by the IRS or a notice from the IRS is received.

5.1.28.13.1  
(07-14-2021)

**Types of BMF Identity  
Theft Processing**

#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#

5.1.28.13.2  
(03-24-2023)

**Research to  
Substantiate BMF  
Identity Theft**

- (1) Prior to validating BMF identity theft, conduct sufficient research to substantiate the identity theft and rule out any other problematic issues, such as a mixed entity. A mixed entity occurs when two or more taxpayers file a tax return for the same period using the same TIN. This may not be identity theft and instead is the result of taxpayer error, return preparer error, or IRS processing error.
- (2) Research the following on IDRS for the entity as appropriate,
- CC NAMEE, CC INOLES
  - CC BMFOLE - reflects a cross reference (XREF) TIN/ITIN or SSN of the entity's responsible party
  - Cross reference EINs and SSNs, parent EIN, successor EIN
  - Filing requirements and filing history
  - Entity establishment date
  - Name/address changes
- (3) Research CC IRPTR for documents filed by the
- Business (including CC IRPTRI for Form W-2s filed)
  - Payers to the business
- (4) Review returns filed using CC TRDBV, CC BRTVU, Modernized e-File (MEF)/ Employee User Portal (EUP), AMS

**Note:** See Exhibit 5.1.28-5, Exhibit 5.1.28-6, and Exhibit 5.1.28-7 for more applicable IDRS research when the taxpayer maintains they never applied for an EIN, or when the entity is active or inactive.

- (5) ESTAB copies of the Form 941 to verify the name and signature on the form.
- (6) Research payment patterns on the Remittance Transaction Register (RTR) for existing payments or the lack of payments
- (7) Review other sources as appropriate such as AMS history and/or Accurant.

**Note:** The required research **must** be performed to support (or disprove) a claim. If identity theft cannot be established through research, refer to IRM 5.1.28.15, BMF Taxpayer Identity Theft Claim, to validate there is a BMF identity theft issue and not a routine account issue.

5.1.28.14  
(07-14-2021)  
**BMF Identity Theft  
Tracking Indicators**

- (1) BMF identity theft indicators are applied if identity theft is highly probable or the determination had been made that identity theft occurred AND the case is controlled into a identity theft treatment stream.
- (2) Review the accounts for prior identity theft indicators before inputting the initial TC 971 AC 522. If the account is already marked with a TC 971 AC 522 IDTCLM, do not input a second code for the same MFT and tax period even if the initial TC 971 AC 522 IDTCLM reflects another BOD/Program.
- (3) BMF identity theft tracking indicators, unlike those used in IMF, are applied to all MFT's and tax periods affected by identity theft. IPSO established three distinctive Tax Administrative Source Codes for BMF accounts:
  - **TC 971 AC 522 IDTCLM**, for the initial allegation or suspicion of identity theft prior to the taxpayer providing their identity theft claim.
  - **TC 971 AC 522 IDTDOC**, when the taxpayer provides a complete and legible identity theft claim.
  - **TC 971 AC 522 CLSIDT**, for BMF case resolved.

5.1.28.14.1  
(03-24-2023)  
**BMF Identity Theft  
Action Code is Routed  
and Processed on Form  
4844**

- (1) Complete Form 4844, Request for Terminal Action, to request input of the BMF identity theft codes and forward to DITA team located as follows:

Email Address	Efax Number	Mailing Address
<i>mailto:*SBSE CCS DITA</i>	1-855-786-6575	Internal Revenue Service DITA Mail Stop 4-J30- 151 2970 Market St., Philadelphia, PA 19104

- (2) The BMF identity theft indicator is input to the MFT and Tax Period affected by the identity theft and will post to TXMOD and BMFOLT. See examples of completed Forms 4844 at Exhibit 5.1.28-3. and Exhibit 5.1.28-4. Complete the applicable blocks of Form 4844, including:
  - a. EIN
  - b. Name control
  - c. MFT code
  - d. Periods
  - e. Name of taxpayer

5.1.28.14.1.1  
(05-15-2014)

**Miscellaneous Field  
Input**

- (1) Complete the three parts of the miscellaneous field

- BOD - "SB"
- Program Name - "FC"
- Tax Administration Source Code - either "IDTCLM", "IDTDOC", or "CLSIDT".

**Example: SB FC IDTDOC**

5.1.28.14.1.2  
(01-11-2016)

**Secondary Date Field**

- (1) Complete the secondary date field as follows:

If requesting	then the secondary date field is the
IDTCLM	date of the taxpayer's allegation or, if you first recognized the taxpayer was the victim of identity theft, the date of that awareness.
IDTDOC	received date of the taxpayer's documents.
CLSIDT	date the identity theft issue was resolved.

5.1.28.14.2  
(06-20-2017)

**Reversing Pending BMF  
Identity Theft Indicators**

- (1) If the taxpayer alleged identity theft, but internal research cannot substantiate the claim and the taxpayer has not provided the requested claim, then complete Form 4844 to request input of TC 972 AC 522 with the tax administration source code **NORPLY** in the miscellaneous field with the BOD and program name.

**Example: SB FC NORPLY**

- (2) If you determine identity theft is not a factor in the case, then complete Form 4844 to request TC 972 AC 522 with the tax administration source code **NOIDT** in the miscellaneous field with the BOD and program name.

**Example: SB FC NOIDT**

- (3) If you determine the original identity theft claim was received fraudulently, then complete Form 4844 to request input of TC 972 AC 522 with the tax administration source code **FALSE** in the miscellaneous field with the BOD and program name.

**Example: SB FC FALSE**

- (4) Enter the secondary date of the TC 971 AC 522 being reversed.

5.1.28.15  
(03-24-2023)

**BMF Taxpayer Identity  
Theft Claim**

- (1) In some instances, taxpayers must provide additional information to establish the fact that they are truly victims of identity theft. The Form 14039-B, Business Identity Theft Affidavit, will be utilized to obtain additional information to support the identity theft claim only if internal/external research cannot validate identity theft. Refer to IRM 25.23.9.7, Form 14039-B, Business Identity Theft Affidavit, for additional information on when to send the form.

**Note:** As of August 1, 2020, Form 14039-B is available online to the general public.

- (2) If unable to resolve the account by using internal information sources and/or by information already provided by the taxpayer, request additional information. Taxpayer information to substantiate identity theft may include:

Taxpayer Information	Description
Authentication of identity	<ul style="list-style-type: none"> <li>IMF - A copy of a valid U.S. federal or state government-issued form of identification to authenticate identity. <b>Example:</b> Driver's license, state identification card, Social Security card, passport, etc. <b>Note:</b> This link provides a list of acceptable primary and secondary forms of identification: <a href="https://www.fedidcard.gov/document/acceptable-forms-id?download=1">https://www.fedidcard.gov/document/acceptable-forms-id?download=1</a></li> <li>BMF - Articles of Incorporation, Articles of Organization, statement from director or officer on business letterhead, trust or estate document.</li> </ul>
Evidence of identity theft	<p>Secure a copy of a police report or Form 14039-B, Business Identity Theft Affidavit</p> <p><b>Note:</b> Form 14039-B should only be requested when the taxpayer has not previously submitted the form or when the submitted form was illegible.</p>
Evidence of business operation	<p>Copy of utility bill, invoice, mortgage or rent receipt or other similar documentation.</p> <p><b>Exception:</b> Evidence of business operation is not needed if the taxpayer never requested or has no knowledge of an EIN.</p>

- (3) Establish a 30-day deadline for the taxpayer to submit a claim and suspend any collection activity.
- (4) An identity theft claim can be accepted from the taxpayer or their representative with Power of Attorney Form 2848, Power of Attorney and Declaration of Representative.
- (5) Secure and handle the claim in the same manner as other sensitive taxpayer information. The documents must be retained with the closed case file.
- (6) Acknowledge receipt of a complete and legible claim within 30 days unless the identity theft claim is received in person.

- (7) When the identity theft claim/additional information have been verified as complete and legible, submit completed Form 4844 to request input of TC 971, AC 522, IDTDOC

5.1.28.16  
(03-24-2023)

**BMF Identity Theft Case Actions**

- (1) The following subsections provide procedures for several BMF identity theft scenarios.
- (2) Use Form 14566, BMF Identity Theft Referral, and forward it through the area identity theft liaison. See the Servicewide Electronic Research Program (SERP) Identity Theft - SBSE Field Collection & OIC (IMF/BMF) webpage, <http://serp.enterprise.irs.gov/content/who-where/identity-theft-sbse-field-collection-and-oic.html> for liaison names and contact information by location.
- (3) All referrals must go through the area's liaison prior to being sent to the SBSE BMF identity theft liaison - Collection Policy. See IRM 5.1.28.17(4) for additional guidance on the referral procedures.

**Note:** Collection employees should follow established procedures to request case assistance from the Collection identity theft liaisons after researching this IRM, or if there is an adjustment issue that requires attention, the employee should ask their manager for guidance and direction. If the employee's manager is unable to answer the questions, the manager should elevate it through the area identity theft liaison to SBSE BMF identity theft liaison - Collection Policy.

- (4) For individual victims of BMF related identity theft, see IRM 25.23.9.4.2, Individual Taxpayers Reporting to be Victims of Business-Related Identity Theft.

5.1.28.16.1  
(03-24-2023)

**Form 941/944 Balance Dues**

- (1) When it is confirmed BMF identity theft occurred and the appropriate transaction codes have been requested, follow the steps in this table to address any refund(s) issued:

If	Then
the Forms 941/944 refund(s) were issued and the perpetrator(s) can be identified	develop a fraud referral and consult with CI before requesting any adjustment to the BMF balance due.
the Forms 941/944 refund(s) were issued and the perpetrator(s) cannot be identified	prepare Form 14566, BMF Identity Theft Referral, to correct the BMF account and forward to the area identity theft liaison, see IRM 5.1.28.16(2) to find your area identity theft liaison.
the Forms 941/944 refund(s) were not issued or the bogus W-2s were not claimed on a Form 941/944	prepare Form 14566, BMF Identity Theft Referral, to correct the BMF account and forward to the area identity theft liaison, see IRM 5.1.28.16(2) to find your area identity theft liaison.

**Exception:** For non-master file cases, forward Form 3870, Request for Adjustment, to the Accounts Management NMF team at:

Cincinnati Campus, CAMC

201 W. Rivercenter Blvd., Stop 6111G, Team C103

Covington, KY 41011

- (2) If you have determined the EIN is fictitious and was established for the sole purpose of defrauding the government through the filing of individual and business false refund returns or income documents, see IRM 5.1.28.17(2), Form 14566, BMF Identity Theft Referral, below.
- (3) If the balance due is the result of an IRS-CAWR or SSA-CAWR assessment (for more information on assessment identification, see IRM 5.1.15.7, Combined Annual Wage Reconciliation (CAWR) Adjustment), then prepare Form 3870, Request for Adjustment, to request abatement of the TC 290 assessment. Attach all information supporting the determination including IDRS research and forward the findings to the CAWR unit using the state mapping guide in Exhibit 5.1.15-3, State Mapping for IRS-CAWR and SSA-CAWR.
- (4) See the example below for suggested wording to write in Item 11 of Form 3870.

**Example:** The following information should be used in Item 11, Reason for Adjustment on Form 3870 as follows:

- IRS-CAWR abatement of tax
  - Requested action: Abate TC 290, dated MM-DD-YYYY in the amount of \$XX
  - Justification: The EIN for this entity is fictitious and was used for the sole purpose of defrauding the government through the filing of false refund returns.
  - Attached: IDRS research
- (5) If the balance due on a BMF return involving identity theft is the result of an SFR assessment with a TC 300, then prepare Form 3870, Request for Adjustment, to request abatement of TC 300.
    - a. For TC 300 assessments with PC (Project Code) 0453, PBC (Primary Business Code) 296 on TXMOD, forward Form 3870, Request for Adjustment, with all information supporting the determination attached to:

Internal Revenue Service

Attn: Team 205/Recon

201 W. Rivercenter Blvd. Stop 8202G

Covington, KY 41011

- b. For all other TC 300 assessments research TXMOD for the PBC (Primary Business Code), SBC (Secondary Business Code) and EGC (Employee Group Code) and locate the manager for the group on this

#  
#

3870 with all information supporting the determination to the manager.

5.1.28.16.1.1  
(07-14-2021)  
**Researching Issued Refunds**

- (1) Access IDRS when researching an issued refund to identify the perpetrator:
  - a. CC IMFOL, CC BMFOL - for a paper check number and issue date
  - b. CC IMFOBT - for IMF electronic refund routing and account number
  - c. CC TRDBV- for the electronic refund routing and account number
- (2) Consult with your fraud technical advisor (FTA) and Area Counsel to determine the appropriate next steps to take.
- (3) See IRM 25.5.6, Summonses on Third-Party Witnesses, when summoning a financial institution for additional information on the refund.

5.1.28.16.2  
(03-24-2023)  
**BMF Bal Dues - Taxpayer's Name and SSN Used by Third Party**

- (1) When it is confirmed that BMF identity theft occurred, the appropriate transaction codes have been requested and the balance dues are for a business operated by a third-party who established the business using a stolen SSN, first consult with Area Counsel.
- (2) If, with Counsel's concurrence, the unpaid liabilities are to be moved to a new EIN, then secure a new EIN for the third-party by preparing a "dummy" Form SS-4, Application for Employer Identification Number, and faxing it to the Cincinnati Internal Use Only.
- (3) Include your name, position, fax, phone number, and any special instructions on the fax cover sheet.
- (4) Prepare Form 12810, Account Transfer Request Checklist, to transfer the assessment to the new EIN and forward to DITA per contact information at IRM 5.1.28.14.1(1).
- (5) Proceed with collection.

#

5.1.28.16.3  
(03-24-2023)  
**Business Tax Return Claiming Refundable Credit**

- (1) In a case involving a BMF refund for a refundable credit where identity theft has been confirmed, and the TC 971 AC 522 requested, take the appropriate actions in this table:

#  
#  
#  
#  
#  
#

If	Then
the refund was issued and the perpetrator can be identified	contact the perpetrator and request the refund be returned.
the perpetrator refuses to return the refund and an assessment has been made against the perpetrator	pursue collection from the perpetrator using available collection tools.
the perpetrator refuses to return the refund and an assessment has been made against the victim	prepare Form 14566 to request the "bad" return be backed out and the credit returned to the account and send the form to the area identity theft liaison. If applicable, pursue collection from the perpetrator using nominee or alter-ego theory. See IRM 5.17.14.7, Nominee, Alter Ego, and Transferee Elements.
the perpetrator refuses to return the refund, no assessment has been made against the perpetrator, the deficiency procedures apply to recover the refund, and jeopardy conditions exist	prepare Form 14566 to request the "bad" return be backed out and the credit returned to the account and send the form to the area identity theft liaison. Pursue collection using jeopardy assessment procedures and jeopardy levy procedures. See IRM 5.1.4, Jeopardy, Termination, Quick and Prompt Assessments and IRM 5.17.15, Termination and Jeopardy Assessments and Jeopardy Collection.
the perpetrator refuses to return the refund, no assessment has been made against the perpetrator, and the refund was obtained by overstating prepayment credits on an income tax return	prepare Form 14566 to request the "bad" return be backed out and the credit returned to the account and send the form to the area identity theft liaison. Pursue a summary assessment against the perpetrator pursuant to IRC 6201(a)(3).

If	Then
the perpetrator refuses to return the refund, no assessment has been made against the perpetrator, and the refund was based on (1) credits for qualified sick leave wages, qualified family leave wages, or qualified family health plan expenses under the Families First Coronavirus Response Act of 2020, or (2) credits for qualified wages under the Coronavirus Aid, Relief, and Economic Security Act of 2020	prepare Form 14566 to request the "bad" return be backed out and the credit returned to the account and send the form to the area identity theft liaison. Pursue a summary assessment against the perpetrator pursuant to 26 CFR 31.3111-6T or 26 CFR 31.3221-5T.
the perpetrator cannot be identified, or the refund was not issued	prepare Form 14566 to correct the account and send the form to the area identity theft liaison, see IRM 5.1.28.14.1(1) for DITA contact information.

- (2) If the EIN on the return is determined to be fictitious, see IRM 5.1.28.17(2) below.

5.1.28.17  
(07-14-2021)  
**Form 14566, BMF  
Identity Theft Referral**

- (1) If you are unable to determine if an EIN is fictitious and you suspect BMF identity theft, submit Form 14566, BMF identity theft referral, through your area identity theft liaison. See IRM 5.1.28.16, BMF Identity Theft Case Actions and follow the steps below:
- Complete Form 14566 using the instructions found in Exhibit 25.23.9-6, BMF Identity Theft Referral Form.
  - Provide specific information that led to the potential for BMF identity theft.
  - Continue to work your case to completion, if possible, without waiting on a response from the BMF identity theft unit.
- (2) If you have determined that the EIN is fictitious and was established for the sole purpose of defrauding the government through the filing of business false refund returns or income documents, refer the EIN on Form 14566 through the area identity theft liaison following the steps below:
- Complete Form 14566 using the instruction found in Exhibit 25.23.9-6, BMF Identity Theft Referral Form.
  - Provide specific information that led to BMF identity theft.
  - Include on your referral the request to have EIN locked with the TC 971 AC 524. Refer to IRM 25.23.9.8.4, Referrals to Lock the Account.
- (3) If false income documents have been filed, forward Form 14566 through the area identity theft liaison to advise Combined Annual Wage Reporting (CAWR). See IRM 25.23.9.8.5, Referrals to Combined Annual Wage Reporting (CAWR), and follow the steps below:
- Complete Form 14566 using the instructions found in Exhibit 25.23.9-6, BMF Identity Theft Referral Form.
  - Provide specific details and documentation if available.

**Note:** Any account adjustments should be requested prior to advising CAWR.

#  
#  
#  
#  
#  
#

**This Page Intentionally Left Blank**

## Exhibit 5.1.28-1 (05-15-2014)

### IMF Form 4844 Example Input of TC 971 AC 522 Pending Claim

<b>Request for Terminal Action</b>	EIN or SSN XXX-XX-XXXX		Name control	MFT code	Periods
	Plan No/Report No (MFT 74, 76 & 46)		XXXX	00	0000
	Name of taxpayer XXXXXXXX XXXXXXXX		Address of taxpayer (if necessary)		
<b>Taxpayer Account Changes</b>	Transaction code	Amount (if applicable)	<b>Control Base Data Request</b>		Remarks
<b>Type of Research Requested</b>			<input type="checkbox"/> ACTON Activity code: _____ Status code: _____ A - Assigned M - Monitor/Other B - Background S - Suspense C - Closed Category code: _____ Employee no.: _____ <input type="checkbox"/> TC 148 Entity indicator: _____		Input TC 971 AC 522 under ENMOD
<input type="checkbox"/> Assessed balance \$ _____ <input type="checkbox"/> Accruals to (Date: mmddyyyy) _____ Interest ..... \$ _____ Penalty ..... \$ _____ Total due ..... \$ _____					
<input type="checkbox"/> Module printout <input type="checkbox"/> Transactions after (Date: mmddyyyy) <input type="checkbox"/> Complete printout <input type="checkbox"/> Other (Specify) _____			Identity Theft Action Code TC 971 AC 522 Miscellaneous Field Input SBSE CFBALDUE PNDCLM Secondary Date Field 12312010		
<input type="checkbox"/> Return DLN _____ <input type="checkbox"/> DLN not available <input type="checkbox"/> Photocopy <input type="checkbox"/> Original <input type="checkbox"/> Form W-2 <input type="checkbox"/> Other (Specify) _____ _____ _____			Employee IDRS number      Name of requester _____ Telephone no. (      ) Signature of requester _____ Date (mmddyyyy)		
			Request Approved      Signature of supervisor (if necessary) <input type="checkbox"/> Yes Request done      Name of Terminal Operator <input type="checkbox"/> Yes      _____ <input type="checkbox"/> No      Telephone no. (      ) Signature of Terminal Operator _____ Date (mmddyyyy)		

Form **4844** (Rev. 11-2011)      Catalog No. 23470Y      publish.no.irs.gov      Department of the Treasury – Internal Revenue Service

## Exhibit 5.1.28-2 (05-15-2014)

## IMF Form 4844 Example Input of TC 972 AC 522 No Identity Theft

<b>Request for Terminal Action</b>	EIN or SSN XXX-XX-XXXX		Name control	MFT code	Periods
	Plan No/Report No (MFT 74, 76 & 46)		XXXX	00	0000
	Name of taxpayer XXXXXXXX XXXXXXXX		Address of taxpayer (if necessary)		
Taxpayer Account Changes	Transaction code	Amount (if applicable)	<b>Control Base Data Request</b>		Remarks
<b>Type of Research Requested</b>			<input type="checkbox"/> ACTON Activity code: _____ Status code: _____ A - Assigned M - Monitor/Other B - Background S - Suspense C - Closed Category code: _____ Employee no.: _____		Input TC 972 AC 522 under ENMOD
<input type="checkbox"/> Assessed balance \$ _____ <input type="checkbox"/> Accruals to (Date: mmddyyyy) _____ Interest ..... \$ _____ Penalty ..... \$ _____ Total due ..... \$ _____			<input type="checkbox"/> TC 148 Entity indicator: _____		
<input type="checkbox"/> Module printout <input type="checkbox"/> Transactions after (Date: mmddyyyy) <input type="checkbox"/> Complete printout <input type="checkbox"/> Other (Specify) _____			Identity Theft Action Code TC 972 AC 522		
<input type="checkbox"/> Return DLN _____ <input type="checkbox"/> DLN not available <input type="checkbox"/> Photocopy <input type="checkbox"/> Original <input type="checkbox"/> Form W-2 <input type="checkbox"/> Other (Specify) _____ _____ _____			Miscellaneous Field Input SBSE CFBALDUE NOIDT		
			Secondary Date Field 12312010		
			Employee IDRS number	Name of requester	Badge number
			Telephone no. (      )		
			Signature of requester		Date (mmddyyyy)
			Request Approved	Signature of supervisor (if necessary)	Date (mmddyyyy)
			<input type="checkbox"/> Yes <input type="checkbox"/> No		
			Request done	Name of Terminal Operator	Badge number
			<input type="checkbox"/> Yes <input type="checkbox"/> No		
			Telephone no. (      )		
			Signature of Terminal Operator		Date (mmddyyyy)

Form 4844 (Rev. 11-2011)

Catalog No. 23470Y

publish.no.irs.gov

Department of the Treasury – Internal Revenue Service

Exhibit 5.1.28-3 (05-15-2014)

BMF Form 4844 Example Input of TC 971 AC 522 Initial Allegation or Suspicion of Identity Theft

<b>Request for Terminal Action</b>	EIN or SSN 00-XXXXXXX		Name control	MFT code	Periods
	Plan No/Report No (MFT 74, 76 & 46)		XXXX	01	201212
	Name of taxpayer XXX XXXXXXX XXXXX		Address of taxpayer (if necessary)		
<b>Taxpayer Account Changes</b>	<b>Transaction code</b>	<b>Amount (if applicable)</b>	<b>Control Base Data Request</b>		<b>Remarks</b>
<b>Type of Research Requested</b>			<input type="checkbox"/> ACTON Activity code: _____ Status code: _____ A - Assigned M - Monitor/Other B - Background S - Suspense C - Closed Category code: _____ Employee no.: _____		Input TC 971 AC 522 IDTCLM
<input type="checkbox"/> Assessed balance \$ _____ <input type="checkbox"/> Accruals to (Date: mmddyyyy) _____ Interest ..... \$ _____ Penalty ..... \$ _____ Total due ..... \$ _____			<input type="checkbox"/> TC 148 Entity indicator: _____		
<input type="checkbox"/> Module printout <input type="checkbox"/> Transactions after (Date: mmddyyyy) <input type="checkbox"/> Complete printout <input type="checkbox"/> Other (Specify) _____			Identity Theft Action Code TC 971 AC 522      Miscellaneous Field Input SB FC IDTCLM      Secondary Date Field 11072013		
<input type="checkbox"/> Return DLN _____ <input type="checkbox"/> DLN not available <input type="checkbox"/> Photocopy <input type="checkbox"/> Original <input type="checkbox"/> Form W-2 <input type="checkbox"/> Other (Specify) _____ _____ _____			Employee IDRS number _____      Name of requester _____      Badge number _____ Telephone no. (      ) _____ Signature of requester _____      Date (mmddyyyy) _____ Request Approved      Signature of supervisor (if necessary)      Date (mmddyyyy) <input type="checkbox"/> Yes Request done      Name of Terminal Operator      Badge number <input type="checkbox"/> Yes      Telephone no. (      ) _____ <input type="checkbox"/> No Signature of Terminal Operator      Date (mmddyyyy) _____		

## Exhibit 5.1.28-4 (05-15-2014)

## BMF Form 4844 Example Input of TC 971 AC 522 Indicator Case Resolved

<b>Request for Terminal Action</b>	EIN or SSN 00-XXXXXXX		Name control	MFT code	Periods
	Plan No/Report No (MFT 74, 76 & 46)		XXXX	01	201212
	Name of taxpayer XXX XXXXXXX XXXXX		Address of taxpayer (if necessary)		

  

<b>Taxpayer Account Changes</b>	Transaction code	Amount (if applicable)	<b>Control Base Data Request</b>		Remarks Input TC 971 AC 522 CLSIDT
			<input type="checkbox"/> ACTON Activity code: _____ Status code: _____ A - Assigned M - Monitor/Other B - Background S - Suspense C - Closed Category code: _____ Employee no.: _____ <input type="checkbox"/> TC 148 Entity indicator: _____		
<b>Type of Research Requested</b>					
<input type="checkbox"/>	Assessed balance	\$ _____			
<input type="checkbox"/>	Accruals to (Date: mmddyyyy)	_____			
	Interest	\$ _____			
	Penalty	\$ _____			
	<b>Total due</b>	\$ _____			
<input type="checkbox"/>	Module printout	<input type="checkbox"/> Transactions after (Date: mmddyyyy)	Identity Theft Action Code TC 971 AC 522		Miscellaneous Field Input SB FC CLSIDT
<input type="checkbox"/>	Complete printout		Employee IDRS number	Name of requester	Badge number
<input type="checkbox"/>	Other (Specify) _____		Telephone no. ( )		
<input type="checkbox"/>	Return DLN _____		Signature of requester		Date (mmddyyyy)
<input type="checkbox"/>	DLN not available		Request Approved		Date (mmddyyyy)
<input type="checkbox"/>	Photocopy <input type="checkbox"/> Original <input type="checkbox"/> Form W-2		Signature of supervisor (if necessary)		
<input type="checkbox"/>	Other (Specify) _____		Request done		Badge number
			<input type="checkbox"/> Yes		
			<input type="checkbox"/> No		
			Name of Terminal Operator		
			Telephone no. ( )		
			Signature of Terminal Operator		Date (mmddyyyy)

Form **4844** (Rev. 11-2011)

Catalog No. 23470Y

publish.no.irs.gov

Department of the Treasury – Internal Revenue Service

## Exhibit 5.1.28-5 (07-14-2021)

### IDRS Research - Taxpayer Never Applied for an EIN

The table below was created to assist you in identifying which command code to use to determine if the taxpayer ever applied for an EIN. Additional research resources for making a BMF identity theft determination are found in Exhibit 25.23.9-7, BMF Identity Theft Research Requirement.

Question	Research
Are there any identity theft indicators already on the account?	CC TXMOD/BMFOLT
Is the business owner a minor, nonfiler, elderly, deceased, an individual with an IMF identity theft indicator, etc.?	CC INOLES, ENMOD
Is there a Form 941 filing requirement?	CC BMFOLE
Were returns filed prior to the entity established date?	CC TXMOD/BMFOLT
Were Forms 1040 refund returns filed using Form W-2?	CC IMFOLI
For a sole proprietor, does the individual file a Schedule C with this EIN?	CC TRDBV
Were payments made under the EIN?	CC BMFOLP
Did other business entities report making payments to the business?	CC IRPTRI

**Exhibit 5.1.28-6 (07-14-2021)**  
**IDRS Research - Active Business**

The table below was created to assist you in identifying which command code to use to determine if the business is active. Additional research resources for making a BMF identity theft determination are found in Exhibit 25.23.9-7, BMF Identity Theft Research Requirement.

Question	Research
Are there any identity theft indicators already on the account?	CC TXMOD/BMFOLT
Any major changes in returns filed, amounts reported, refundable credits claimed from prior years?	CC TXMOD/BMFOLT
Was there more than one submission of Forms W-2?	CC BMFOLU
Recent change in address from previous returns filed?	CC BRTVU/TRDBV
Is there an adjustment on the account, e.g., CAWR, Examination?	CC TXMOD/BMFOLT
Is the preparer on the return in question different from the one used on prior year returns?	CC TRDBV
Do the total payments posted on the IDRS module match those on the return?	CC BRTVU/TRDBV

**Exhibit 5.1.28-7 (07-14-2021)**  
**IDRS Research - Inactive Business**

The table below was created to assist you in identifying which command code to use to determine if the business is inactive. Additional research resources for making a BMF identity theft determination are found in Exhibit 25.23.9-7, BMF Identity Theft Research Requirement.

Question	Research
Are there any identity theft indicators already on the account?	CC TXMOD/BMFOLT
Was a final return filed?	CC BMFOLE
Are there any open filing requirements?	CC BMFOLE
Any major changes in returns filed, amounts reported, refundable credits claimed from prior years?	CC TXMOD/BMFOLT
Was there a significant amount of inactivity prior to the filing?	CC TXMOD/BMFOLT
Were Forms 1040 refund returns filed using Form W-2?	CC IMFOLI
Were payments made under the EIN?	CC BMFOLP

