



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

25.23.11

SEPTEMBER 9, 2024

EFFECTIVE DATE

(10-01-2024)

PURPOSE

- (1) This transmits revised IRM 25.23.11, Business Master File (BMF) Identity Theft Procedures for Accounts Management

MATERIAL CHANGES

- (1) IRM 25.23.11.1 - (3) Updated to correct directorship. IPU 24U0647 issued 05-14-2024
- (2) IRM 25.23.11.1.2 - (4) Added TAS verbiage to current standard language per TAS.
- (3) IRM 25.23.11.6 - (2) Updated Box 3 to correct linked IRM for accounts in Status 26. Updated Box 8 to correct linked IRM 25.23.11.6.5(7) to (9). IPU 24U0647 issued 05-14-2024
- (4) IRM 25.23.11.6.3 - (11) New paragraph regarding Business Tax Accounts (BTA) and actions to take if the taxpayer calls stating they cannot access BTA and/or Energy Credit Online (ECO) tool when RICS and/or AM BMF IDT have determined the EIN to be fabricated. Subsequent paragraphs were renumbered. (12) Added information throughout regarding address changes and added a note to Box 6 regarding where to see case determinations made by RICS. (13) Box 3 - Clarified the referral type to use when sending a referral to RICS. Box 7 - Updated the "If" column for clarity and updated the "Then" column to include the tax year of the referral in the subject line of the secure e-mail. IPU 24U0647 issued 05-14-2024
- (5) IRM 25.23.11.6.3 - Added new (7) with If/Then chart to illustrate the codes and actions RICS takes based on their determinations. Row 3 contains information regarding TC 971 with new AC 717, to post the return and freeze the refund with TC 810 RC 8 (-Q freeze). Moved information from prior paragraphs 7-10 into the chart, and subsequent paragraphs were renumbered. (8) Updated Row 1 to include instructions for after the 60 day timeframe has passed. (9) Added "Note" to Row 2 and expanded the "Note" in Row 6 to explain that RICS does not send determination letters for Entity Fabrication or ID theft determinations. Added new Row 7 and Row 8 for when the taxpayer submits additional information for reconsideration for RICS determination and calls to check on the status. (10) Row 1 - Added fax number to route responses to Letter 6042C if received in CII inventory. Row 6 - Added AC 717 and removed TC 570 and -R freeze information. Row 7 - Added a 'Note' to clarify that if a case includes CI involvement, the referral must include the account has CI involvement.
- (6) IRM 25.23.11.6.3.1 - Renamed subsection from *BMF Returns with CARES Act Credits - AM BMF Identity Theft Teams Only* to *BMF Accounts with RICS and/or IDT Involvement - AM BMF Identity Theft Teams Only* and updated throughout to update references of CARES Act credits to RICS involvement. (4) Added new box 4 regarding -A Freeze and the identity theft issue has been resolved. (5) Added new paragraph and If/Then chart for actions to take regarding reconsiderations of EINs deemed fabricated by AM BMF Identity Theft when the taxpayer cannot access BTA and/or ECO. IPU 24U0647 issued 05-14-2024
- (7) IRM 25.23.6.3.1 - (4) Row 4 - Updated to include research requirement to determine if the TC 150 posted to the account is the taxpayer's valid return. Row 5 - Added new row for when research indicates the TC 150 posted to the account is not the taxpayer's valid return after RICS has made an IDT determination and the account has not been deemed fabricated. Updated the chart throughout to include instructions to remove "Potential Fab EIN" or "Identity Theft" from the sort name line prior to transmitting Letter 916C.

- (8) IRM 25.23.11.6.4 - (2) Updated Step 5 to clarify where to send Form 14566, BMF Identity Theft Referral, and added to include the tax year of the referral in the subject line of the secure email. IPU 24U0647 issued 05-14-2024
- (9) IRM 25.23.11.6.5 - (3) Updated the question regarding home care services when the taxpayer calls and has no knowledge of the EIN or business account. (9) Step 1 - Added to include the tax year of the referral in the subject line of the secure e-mail. IPU 24U0647 issued 05-14-2024
- (10) IRM 25.23.11.6.5 - (1) Incorporated information from IRM 25.23.11.6.5.1, CSR Telephone Guidance for Form 14039-B, prior (1) and prior (2) to provide additional clarification and guidance regarding taxpayer contacts. (3) Strengthened language for clarity and understanding. (5) Added link to IRM 25.23.11.6.5.1, CSR Telephone Guidance for Form 14039-B, if the taxpayer requests assistance completing Form 14039-B.
- (11) IRM 25.23.11.6.5.1 - (2) Clarified 1st bullet regarding individual taxpayers reporting business-related identity theft. IPU 24U0647 issued 05-14-2024
- (12) IRM 25.23.11.6.5.1 - Reformatted entire section for clarity and understanding. Incorporated information from prior (1) and (2) into IRM 25.23.11.6.5. Prior (3) 'How to Complete the Form' moved into table format in new (2). Prior (4) 'Submitting Form 14039-B' moved into new (3) and (4).
- (13) IRM 25.23.11.6.6.1 - (3) Updated the table to clarify procedures when requesting an account be locked with TC 971 AC 524. A PDF print of the original entity (CC ENMOD), including filing requirements, is now required. A reminder for EO employees working IDT was also added. (4) Added table to provide guidance when requesting an account be unlocked with TC 972 AC 524. (6) Removed "BMF IP" from the literal in the MISC field of TC 971 AC 524 when RICS locks an account suspected of being fabricated with EINFB2. IPU 24U0647 issued 05-14-2024
- (14) IRM 25.23.11.6.6.1 - Renamed subsection from "Fabricated EIN Referrals" to "Fabricated EINs" and reformatted for clarity and understanding. Subsection now clearly defines what is applicable to all AM BMF CSRs and what is applicable only to AM BMF CSRs trained in BMF Identity Theft. Incorporated information from prior (6) into new paragraphs (3), (5), and (6). Added new information regarding fabricated EINs and new If/Then chart in (4) for inquiries received on paper or phone call and the account is already deemed fabricated. Due to restructuring, paragraphs have been renumbered.
- (15) IRM 25.23.11 revised throughout to update organizational title Wage and Investment to Taxpayer Services. Various editorial changes have been made throughout the IRM. Reviewed and updated grammar, web addresses, form names, organizational terms , and IRM references where applicable. IPU 24U0647 issued 05-14-2024

EFFECT ON OTHER DOCUMENTS

IRM 25.23.11, Business Master File (BMF) Identity Theft Procedures for Accounts Management effective 10-01-2023 is superseded. The following IRM Procedural Update (IPU) issued on May 14, 2024 has been incorporated into this IRM: 24U0647.

AUDIENCE

The provisions in this manual apply to all Accounts Management employees working BMF identity theft cases.

LuCinda Comegys
Director, Accounts Management
Taxpayer Services Division

25.23.11

Business Master File (BMF) Identity Theft Procedures for Accounts Management

Table of Contents

25.23.11.1 Program Scope and Objectives

25.23.11.1.1 Background

25.23.11.1.2 Authority

25.23.11.1.3 Responsibilities

25.23.11.1.4 Acronyms/Definitions

25.23.11.1.5 Related Resources

25.23.11.1.6 Business Master File (BMF) Identity Theft Overview

25.23.11.2 What is Business Master File (BMF) Identity Theft (IDT)?

25.23.11.3 Fraud vs Business Master File (BMF) Identity Theft

25.23.11.4 Business Master File (BMF) ID Theft Research

25.23.11.4.1 Accounts containing TC 130

25.23.11.5 Business Master File (BMF) Identity Theft Indicators

25.23.11.6 Business Master File (BMF) Identity Theft Inquiries

25.23.11.6.1 Non-Tax Related Identity Theft

25.23.11.6.2 Individual Taxpayers Reporting to be Victims of Business-Related Identity Theft

25.23.11.6.3 BMF Returns Selected for RICS Review

25.23.11.6.3.1 BMF Accounts with RICS and/or IDT Involvement - AM BMF Identity Theft Teams Only

25.23.11.6.4 BMF Identity Theft Paper Inquiry

25.23.11.6.5 BMF Identity Theft Phone Inquiry Made to a BMF AM CSR

25.23.11.6.5.1 CSR Telephone Guidance for Form 14039-B

25.23.11.6.6 BMF Identity Theft Referrals - AM BMF Identity Theft Teams Only

25.23.11.6.6.1 Fabricated EINs

25.23.11.6.6.2 Collection Activity - Form 13794 Additional Actions Required - Lien -AM BMF Identity Theft Teams only

25.23.11.6.7 Account Actions - AM BMF Identity Theft Teams Only

25.23.11.6.8 Invalid Return Posted First and the Valid Return is a Balance Due

25.23.11.6.9 Lost Refund

25.23.11.6.10 Reversing TC 130

25.23.11.6.11 Reversing BMF Identity Theft Indicators

Exhibits

25.23.11-1 Accounts Management Form 14566 Instructions

25.23.11.1
(05-14-2024)
Program Scope and Objectives

- (1) **Purpose:** This manual provides case procedures for use when working Accounts Management (AM) Business Master File (BMF) identity theft inventory and providing assistance to victims of identity theft.
- (2) **Audience:** The primary users of the IRM are all Accounts Management employees who are in contact with taxpayers by telephone, correspondence, or in person with business-related identity theft.
- (3) **Policy Owner:** Identity Protection Strategy and Oversight (IPSO) owns the policy relating to Business Master File identity theft under the directorship of Accounts Management.
- (4) **Program Owner:** Identity Theft Victim Assistance (IDTVA) is the internal organization that is responsible for the administration, procedures, and updates related to Accounts Management Business Master File identity theft.
- (5) **Program Goals:** This IRM aims at quickly and effectively resolving Business Master File (BMF) accounts where identity theft is claimed or identified. This IRM outlines the steps to provide relief to those taxpayers whose accounts have been affected by identity theft.

25.23.11.1.1
(10-01-2020)
Background

- (1) Business Master File (BMF) Identity Theft can involve the use of identifying information about a business to file fraudulent returns to support Individual Master File (IMF) identity theft or to obtain refunds from BMF accounts. An individual's stolen personal information can also be used to obtain an Employer Identification Number (EIN) which is used to file false BMF tax returns and income documents. BMF accounts includes the following entity types: sole proprietorship, corporation, partnership, estate, trust, exempt organization, or government entity.

25.23.11.1.2
(10-01-2024)
Authority

- (1) The Taxpayer Bill of Rights (TBOR) lists rights that already existed in the tax code, putting them in simple language and grouping them into 10 fundamental rights. Employees are responsible for being familiar with and acting in accord with taxpayer rights. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For additional information about the TBOR, see www.irs.gov/taxpayer-bill-of-rights.
- (2) Policy Statement 10-1, *Assisting Taxpayers who Report they are Victims of Identity Theft* See IRM 1.2.1.17, Policy Statements for Security, Privacy and Assurance Activities.
- (3) The statutory authority for the Fraudulent Return Request (FRR) is IRC 6103(e), *Disclosure to Persons Having Material Interest*, which provides a listing of persons who may generally request and receive returns and return information. IRC 6103(e)(1)-(6) and IRC 6103(e)(10) concern disclosure of returns. IRC 6103(e)(7) through (e)(9) as well as (e)(11) refer to disclosure of "return information."
- (4) The *Taxpayer Advocate Service* (TAS) is an **independent** organization within the Internal Revenue Service (IRS), led by the National Taxpayer Advocate, that helps taxpayers and protects taxpayer rights. TAS offers free help to taxpayers when a tax problem is causing a financial difficulty, when they've tried and been unable to resolve their issue with the IRS, or when they believe an IRS system, process, or procedure just isn't working as it should. TAS strives

to ensure that every taxpayer is treated fairly and knows and understands their rights under the *Taxpayer Bill of Rights*. TAS has at least one taxpayer advocate office located in every state, the District of Columbia, and Puerto Rico.

25.23.11.1.3
(10-01-2020)
Responsibilities

- (1) All AM employees who take phone calls or work paper cases, where the taxpayer states they are a victim of BMF ID theft or the employee identifies BMF ID theft, are responsible for following the procedures set forth in this IRM.
- (2) Additional information is found in IRM 1.1.13.7.3, Accounts Management, and IRM 21.1.1, Accounts Management and Compliance Services Overview.

25.23.11.1.4
(10-01-2020)
Acronyms/Definitions

(1) **Acronyms**

- ACSS - Automated Collection System Support
- AM - Accounts Management
- AMS - Accounts Management Services
- AUR - Automated Underreporter
- BITR - BMF ID Theft Research Tool
- BMF - Business Master File
- BOD - Business Operation Division
- CC - Command Code
- CII - Correspondence Imaging Inventory
- CSCO - Compliance Services Collection Operations
- CSR - Customer Service Representative
- DOD - Date of Death
- EIN - Employer Identification Number
- FRR - Fraudulent Return Request
- IAT - Integrated Automation Technologies
- IDRS - Integrated Data Retrieval System
- IDT- Identity Theft
- IDTVA - Identity Theft Victim Assistance
- IMF - Individual Master File
- IPSO - Identity Protection Strategy and Oversight
- IRM - Internal Revenue Manual
- IRS - Internal Revenue Service
- LLC - Limited Liability Company
- NMF - Non Master File
- PII - Personally Identifiable Information
- RICS - Return Integrity and Compliance Services
- RIVO -Return Integrity & Verification Operation
- RPM - Return Preparer Misconduct
- SERP - Servicewide Electronic Research Program
- SFR - Substitute For Return
- SSN - Social Security Number
- TAS - Taxpayer Advocate Service
- TC - Transaction Code

(2) **Definitions**

- BMF Identity Theft- BMF IDT is defined by the filing of a Business Tax Return when someone creates, uses, or attempts to use a business' identifying information without authority to obtain tax benefits.
- Fabricated EIN- This is an EIN established for the sole purpose of defrauding the government by the filing of individual Tax Returns or used

for other illicit activities not related to the filing of federal tax returns or other forms. The associated Personally Identifiable Information (PII) may be stolen personal data.

- Fraud- Fraud is when a true owner of the EIN or authorized party attempts to file false tax documents to receive a refund, reduce a tax liability, or receive other tax benefits to which they are not entitled.
- Tax impact- The ID theft has caused a direct effect to the taxpayer's account. This can include the filing of fraudulent tax returns or income documents.
- Non-Tax impact- The business's information has been stolen but currently there is no direct effect on the taxpayer's account.

25.23.11.1.5
(10-01-2020)

Related Resources

- (1) Conduct thorough research when resolving account issues. While not all inclusive, the following resource list may be helpful when researching account issues:

- IRM Part 21, Customer Account Services
- IRM 25.23.9, BMF Identity Theft Processing
- IRM 20.1, Penalty Handbook
- IRM 20.2, Interest
- IRM 25.6.1, Statute of Limitations Processes and Procedures
- IRM 1.2.1.2.36, Policy Statement 1-236, Fairness and Integrity in Enforcement Selection
- Pub 1, Your Rights as a Taxpayer
- IAT BTR Tool, Integrated Automation Technologies Business Identity Theft Research Tool

25.23.11.1.6
(01-22-2020)

Business Master File (BMF) Identity Theft Overview

- (1) This IRM provides procedural guidance for BMF Accounts Management (AM) personnel authorized to research and process BMF Identity Theft (IDT) phone and paper inquiries.
- (2) BMF IDT inquiries are complex and require extensive research. IRM 25.23.9, BMF Identity Theft Processing, provides Servicewide guidance for working cases. BMF taxpayers are often not aware their identities have been compromised until a notice is received from the IRS. The taxpayer may contact IRS after receiving an unexpected notice regarding an inactive employer identification number (EIN), a recently-established EIN they have no knowledge about, or a balance due notice for a BMF form they never filed with the IRS.

Caution: What appears to be a BMF IDT case may actually be an inadvertent misuse of the EIN (e.g., mixed entity, tax return preparer error, etc.) or fraudulent filing by the EIN owner. This is why thorough research must be completed prior to inputting the ID theft indicator or referring the case to another inventory.

- (3) Generally, individual identity theft victims contact the IRS as they attempt to file the current year income tax return and discover that someone else has already filed a return using their taxpayer identification number. However, it may be several years before a business victim becomes aware of criminal activity and contacts the IRS.

25.23.11.2
(10-01-2022)
What is Business Master File (BMF) Identity Theft (IDT)?

- (1) BMF identity theft (IDT) is defined as creating, using, or attempting to use a business’s identifying information to obtain a tax benefit without authority.
- Caution:** There must be a federal tax related impact (e.g., balance due, fraudulent refund issued, Taxpayer Delinquency Investigation (TDI), etc.) before BMF IDT can be considered. Examples of tax related impact include (this list is not all inclusive)
 1. Fraudulent returns filed. This includes original or amended returns
 2. Fraudulent income documents filed by an unauthorized party. This would include Form W-2, Form 1099, etc.

Note: The taxpayer stating, “I did not make this income” does not always mean the case is identity theft. Complete research must be performed per IRM 25.23.9.4, Business Master File (BMF) Identity Theft Research (Inquiry Received via Paper or Phones) and Exhibit 25.23.9-7, Business Master File (BMF) Identity Theft Research Requirement.

If there is no tax related impact, see IRM 25.23.11.6.1, Non-tax Related ID Theft.

- (2) The Service has identified potential ID theft scenarios (this list is not all inclusive):
- ID thief files a fraudulent return to obtain a refund or
 - ID thief files fraudulent return or returns to support fraudulent individual identity theft filings

Note: Be careful to watch for taxpayers who may claim BMF IDT to avoid paying taxes. This is not ID theft.

- (3) The following scenarios provide examples of BMF IDT:

#

[illegible]

- (1) The fraudulent filing of a return or document allowing the filer to receive a refund on an existing account when the filer has the authority to file a tax return on behalf of the business is **not** considered BMF identity theft (IDT). Making the distinction between BMF IDT and fraud by an authorized party can be very difficult.
- (2) Scenario with example of fraud - The filing of a corporate income tax return with refundable credits by an authorized party may be considered fraudulent activity.

##

##

- (4) If the determination is that the fraudulent return has been filed by an authorized party and it is not a case of ID theft, complete Form 14566, BMF Identity Theft Referral, and e-mail to the AM BMF liaison mailbox, *TS AM BMF IDT, to be forwarded to the Frivolous Return Misconduct Program (FRP) for review. Make sure to include the rationale behind the determination. Do not close the case until the review is complete.

25.23.11.4
(10-01-2023)
**Business Master File
(BMF) ID Theft Research**

- (1) It is essential to complete all account research prior to taking any account actions, transferring a call or reassigning a case. The initial Customer Service Representative (CSR) is responsible for researching the account to eliminate any routine account issues and placing a potential BMF IDT inquiry into the appropriate work stream. The *Integrated Automation Technologies (IAT) BMF Identity Theft Research (BITR) Tool* should be used for research when possible.
- (2) Complete all research to rule out the potential mixed entity/period or other account situations. Use IRM 25.23.9.4, BMF Identity Theft Research (Inquiry received via paper or phones) and Exhibit 25.23.9-7, BMF Identity Theft Research Requirement, as a research guide.
- (3) Document the findings on CII or AMS that support the suspected ID theft claim.
- (4) The examples below are possible research paths that may need to be considered prior to making a BMF IDT determination:
- Example 1:** The taxpayer received an unexpected balance due notice and claims no knowledge of the tax return and/or business account. The balance due may have been created by an inadvertent tax return filing, return preparation error, IRS processing error, or another entity using the same employer identification number (EIN). An explanation of the balance due may need to be provided to the taxpayer. Review the entity section of the documents and determine who signed the returns. If the taxpayer signed the returns, forward copies of these documents to the taxpayer for review.
 - Example 2:** The taxpayer has an active or inactive business but did not file the return generating the balance due or refundable credit. The balance due may have been created by an inadvertent tax return filing, return preparation error, 6020(b) submission, Substitute For Return (SFR) submission, IRS processing error, or another entity using the same EIN.
 - Example 3:** The account only has one or two Form 941, Employer's Quarterly Federal Tax Return, modules in balance due status without any payments. The taxpayer claims no knowledge of the business and did not request an EIN. Use Command Code IRPTR with definer I to determine whether Forms W-2 were filed for the business. One or two Form 941 modules in balance due (no payments) with matching Form W-2 data may be a sign of BMF IDT.
- (5) Research should include (this list is not all inclusive):

##

- b. Research any payments on the account. This might provide additional information. Utilize RTR to research for paper checks and CC EFTPS for electronic payments. If the taxpayer states they did not make the payment and it cannot be determined where the payment belongs, do not leave the payment on the account. Move the payment to excess if unable to determine where it belongs. On continuous payments that the taxpayer claims they did not make, review CC RFINK for current reporting agent. It may be necessary to contact Ogden EFTPS group to determine which batch filer made the payments if there are no reporting agents on CC RFINK.
- c. Review all case histories on CII and AMS for prior taxpayer contacts. This includes a review of prior closed CII IMF and BMF cases for the EIN.

[illegible]

- 25.23.11.4**

25.23.11.4.1
(09-13-2017)

Accounts containing TC 130

- (1) If there are balances owed resulting from BMF ID theft, research for BMF ID theft to determine the effects it has had on the IMF side of the X-REF SSN owner.
- (2) This would involve reviewing the account to determine if there is a TC 130 on the IMF entity. The posting of a TC 130 stops any overpayments from offsetting or refunding from the account. A V- freeze (outstanding liability freeze) will be set and there may be refunds being held on the account.
- (3) Research all associated accounts for outstanding balances. Balance due accounts can also reside on the Non-master File (NMF) accounts as well. Indications that there is a NMF account are:
 - a. TC 130 in blocking series (BS) 200-299.
 - b. M- freeze. The module balance will appear to be zero. This is caused by the posting of the TC 400 with a false credit which brought the balance to zero. The balance was then moved to NMF.

TC 400 with BS of	Indicates
00	A transfer from MF to NMF
05	Offer in compromise, MF to NMF
09	A transfer from MF to NMF but is a special project
99	An overflow account necessitating a move to NMF

- (4) If the resolution of the ID theft issue will alleviate the balance on the BMF account, research the IMF Non-master File (NMF) account to determine if there any other possible balances are owed by the taxpayer. Use CC TXMOD, SUMRY and ENMOD with definer "N" after the TIN to research the NMF.
- (5) If the determination is made that this is a fabricated EIN and the SSN owner has no association with the business, the TC 130 relating to the business must be reversed.
- (6) If dealing with a legitimate business but BMF ID theft did occur, ensure there are no outstanding liabilities for the business prior to reversing the associated TC 130.
- (7) For procedures to reverse any TC 130 relating to the ID theft, See IRM 25.23.11.6.10, Reversing TC 130.

25.23.11.5
(10-01-2023)

Business Master File (BMF) Identity Theft Indicators

- (1) BMF ID theft indicators are used to track the progress of an ID theft claim.
- (2) Once it is determined there is a high probability of ID Theft or the determination has been made that identity theft has occurred AND the case is controlled into an ID Theft treatment stream, the indicator should be input. Input the indicators only if there is tax related impact, such as fraudulent returns or income documents filed.
- (3) To input the ID theft indicator, use *IAT BTR Tool* and Command Code (CC) REQ77 initiated from TXMODA, when BTR Tool is unavailable. The BMF indi-

cators work differently from IMF indicators as the TC 971 AC 522 does not appear on the entity. Ensure the secondary date and "MISC" sections are correctly input. Indicators must be input on all MFTs and tax periods where ID theft is suspected and/or confirmed.

Note: The Secondary Date field will reflect the IRS receive date or the date of the taxpayer's inquiry. (Due to a programming issue if using today's date and you receive an error message, use the prior day's date). If the identity theft issue was internally identified, use the date you recognized the taxpayer was a victim of identity theft. The ID theft indicators are only input on the TXMODA not the entity section.

Exception: RICS systemic selections for potential BMF IDT review do not contain a secondary date.

Note: MISC- In the MISC field enter WI AM XXXXXX. See below for the definitions of the tax administration codes to be used. See IRM 25.23.9-1, TC 971 AC 5XX - MISC Codes

Action Code	Tax Administration Code	Definition
522	IDTCLM	No taxpayer documentation provided. Research has established ID theft exists or there is a high probability that ID theft exists, refer to IRM 25.23.9.6.1 , <i>Allegation or Suspicion of BMF Identity Theft - TC 971 AC 522 IDTCLM</i> , for additional information. Taxpayer may still need to complete Form 14039-B.

Action Code	Tax Administration Code	Definition
522	IDTDOC	Taxpayer provided a Form 14039, Identity Theft Affidavit or Form 14039-B, Business Identity Theft Affidavit or, Taxpayer Supporting Documentation. For additional information see IRM 25.23.9.6.2, Taxpayer Supporting Documentation-TC 971 AC 522 IDTDOC. If a loose Form 14039-B is received and no TC 971 AC 522 IDTCLM is on the module, input only the TC 971 AC 522 IDTDOC to indicate ID theft claim received from taxpayer.
522	CLSIDT	BMF ID theft case resolved and was confirmed IDT. Refer to IRM 25.23.9.6.3, Closing BMF Identity Theft Issues - TC 971 AC 522 CLSIDT, for additional information.
524	EINFAB	EIN is fabricated and the account has been locked. Send referral to the AM BMF liaison mailbox, <i>*TS AM BMF IDT</i> , if it is determined the entity is fabricated.

- (4) When the input of the TC 971 AC 524 posts it will generate the posting of the TC 020 on the entity and lock the account. The TC 020 will post one cycle after the TC 971 AC 524 and is only visible on CC BMFOLE. A TC 020 generated by a TC 971 AC 524 will not delete the entity but will prevent the posting of returns and payments to a tax module that is not already established on BMF. Refer to IRM 25.23.9-1, Transaction Code (TC) 971 Action Code (AC) 5XX - Misc Codes, for additional tax administration source codes and their descriptions that may be used for locking EIN accounts.
- (5) For the input of the TC 971 AC 524, send the completed referral form and e-mail to the AM BMF liaison mailbox, **TS AM BMF IDT*. On the subject line enter: TC 971 AC 524, and CII Case ID if available. Refer to IRM 25.23.9.8.4, Referrals to Lock the Account. Be certain to include on the referral all appropriate research completed. Document the sending of the referral on AMS along with the details of the request. If working a CII case, attach the referrals to the

Business Master File (BMF) Identity Theft Procedures for Accounts Management 25.23.11

page 11

CII case. If the account has been locked in error, send a referral to the AM BMF liaison mailbox, **TS AM BMF IDT*, to have the TC 971 AC 524 reversed.

- (6) If a TC 971 AC 522 indicator has been placed on the account and after research it is determined that ID theft does not exist, reverse the indicator per IRM 25.23.9.6.5, Reversing BMF Identity Theft Indicators.

25.23.11.6
(05-14-2024)
**Business Master File
(BMF) Identity Theft
Inquiries**

- (1) Once the required research is completed and ID theft is confirmed or there is a high probability ID theft exists, it is necessary to determine whether the case should remain in AM inventory or be referred to another function.
- (2) Use the table below to determine whether the case will remain in AM or be transferred to another function. This initial step is vital to ensure the case is placed in the appropriate identity theft treatment stream as soon as possible.

Reminder: All referrals will go liaison to liaison. All AM referrals will go through the AM BMF ID theft liaison first. The AM BMF ID theft liaison will forward to the appropriate referring function. To find a list of the functional liaisons, see the *BMF ID Theft Liaisons* located on the BMF ID Theft Website on SERP.

	If...	Then...	Additional Information...
1.	If a case is closed in AM with a BMF IDT indicator (TC 971 AC 522, with IDTCLM, IDTDOC, CLSIDT, NORPLY, NOIDT, IRSERR, FALSE, or OTHER) on the tax module	Reassign or refer the case to the assigned or closing CSR. AM only cases	
2.	One or more of the account modules are in Status 22 and completed research indicates potential ID theft	Forward the case to the team leadership for case review and referral approval. If the referral is approved, refer the case to the AM BMF IDT Liaison. Prepare Form 14566, BMF Identity Theft Referral, and send it by secure e-mail to <i>*TS AM BMF IDT</i> . See Exhibit 25.23.11-1, Accounts Management Form 14566 Instructions , for completion details.	<i>Doc 6209 Section 8A-3, MF and IDRS Collection Status Codes</i>

	If...	Then...	Additional Information...
3.	One or more of the account modules are in Status 26 and completed research indicates potential ID theft	Forward the case to the team leadership for case review and referral approval. If the referral is approved, refer the case to the AM BMF IDT Liaison. Prepare Form 14566, BMF Identity Theft Referral, and send it by secure e-mail to <i>*TS AM BMF IDT</i> . See Exhibit 25.23.11-1, Accounts Management Form 14566 Instructions, for completion details.	If there are tax periods in notice status 21 or 58, in addition to the status 26 module(s), input CC STAUP 22 01 to accelerate those tax periods to Status 26. See IRM 21.3.3.4.8.2(4), Campus Collection Function Correspondence/Inquiry/Notice, and <i>Doc 6209 Section 8A-3, MF and IDRS Collection Status Codes</i> for additional information.
4.	There is an open or closed audit, and completed research indicates there is potential ID theft relating to the audit	Forward the case to the team leadership for case review and referral approval. If the referral is approved, refer the case to the AM BMF IDT Liaison. Prepare Form 14566, BMF Identity Theft Referral, and send it by secure e-mail to <i>*TS AM BMF IDT</i> . See Exhibit 25.23.11-1, Accounts Management Form 14566 Instructions, for completion details.	Prior to forwarding to Exam, input TC 470 to prevent erroneous balance due notices from being issued while the case is under review. Refer to <i>Doc 6209 Section 8A-3, MF and IDRS Collection Status Codes</i> for additional information.
5.	The module shows Combined Annual Wage Reporting (CAWR) function activity and completed research indicates there is potential ID theft relating to the CAWR issue	Forward the case to the team leadership for case review and referral approval. If the referral is approved, refer the case to the AM BMF IDT Liaison. Prepare Form 14566, BMF Identity Theft Referral, and send it by secure e-mail to <i>*TS AM BMF IDT</i> . See Exhibit 25.23.11-1, Accounts Management Form 14566 Instructions, for completion details.	Prior to forwarding to CAWR, input TC 470 to prevent erroneous balance due notices from being issued while the case is under review. Refer to <i>Doc 6209 Section 8A-3, MF and IDRS Collection Status Codes</i> for additional information.
6.	The module shows Federal Unemployment Tax Act (FUTA) activity, and completed research indicates there is potential ID theft relating to the FUTA issue	Forward the case to the team leadership for case review and referral approval. If the referral is approved, refer the case to the AM BMF IDT Liaison. Prepare Form 14566, BMF Identity Theft Referral, and send it by secure e-mail to <i>*TS AM BMF IDT</i> . See Exhibit 25.23.11-1, Accounts Management Form 14566 Instructions, for completion details.	Prior to forwarding to FUTA, input TC 470 to prevent erroneous balance due notices from being issued while the case is under review. Refer to <i>Doc 6209 Section 8A-3, MF and IDRS Collection Status Codes</i> for detailed information.

	If...	Then...	Additional Information...
7.	RICS- See IRM 25.23.11.6.3, BMF Returns Selected For RICS Review	1. For paper cases: Refer to IRM 25.23.11.6.3 for procedures before forwarding the case to the team leadership for case review and referral approval. If the referral is approved, forward the case to RICS Unit, OSC Stop 9002. 2. For phones: Refer to IRM 25.23.11.6.3 for procedures.	Do not advise them to submit a Form 14039-B
8.	None of the conditions above are met,	The case will remain in AM and extensive research must be performed to rule out other account issues. If there is a high probability of ID theft and you are untrained in ID theft, contact your team lead to complete a Form 14566 and forward to the appropriate AM ID theft unit per IRM 25.23.11.6.4, BMF Identity Theft Paper Inquiry or IRM 25.23.11.6.5(9)(1), BMF Identity Theft Phone Inquiry Made to a BMF AM CSR.	

Do not refer the case if the ID theft issue is not related to the function's issue.

Example: There is a closed audit and a TC 300 on the account creating a balance due. An amended return comes in requesting a large refund from refundable credits. The ID theft issue is not related to the audit. The case should not be referred to Exam just because there is a TC 300 on the module. Review the ID theft claim and determine if it is related to an issue in another function prior to referring it.

25.23.11.6.1
(10-01-2022)

Non-Tax Related Identity Theft

- (1) If the taxpayer states they are a victim of ID theft and research determines there is no tax related impact, provide the following guidance as applicable.
- (2) If the taxpayer states they were alerted that their Personally Identifiable Information (PII) was breached, refer to IRM 25.23.1.7, Taxpayers who are Victims of a Data Breach, for additional information.
- (3) If the business has experienced a breach of employee or client data, and the taxpayer is seeking assistance for their employees or clients, see IRM 25.23.1.6, Data Breach- Business Entities Whose Employees or Clients PII was Breached, for information to provide the taxpayer.
- (4) If the taxpayer is seeking advice about the data breach of the business, ask the taxpayer about the type of information breached.

25.23 Identity Protection and Victim Assistance

1. If a business or payroll company contacts the Service to report a data loss relating to Forms W-2 information, advise them to go to [IRS.gov](https://www.irs.gov) and search using key word, "Identity Theft". Click on "Identity Protection: Prevention, Detection and Victim Assistance". Click on "Taxes. Security. Together." In the section under "How Businesses Can Help," click on "Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers". This link provides the information on various agencies and how to contact them to report the loss.
2. If a business or payroll company contacts the Service to report a theft in their office that could lead to a data breach but does not include W-2 information, advise them to contact their local stakeholder liaison. The stakeholder liaison listing can be found on [IRS.gov](https://www.irs.gov), search keywords "Stakeholder Liaison" then click on "Stakeholder Liaison Local Contacts". The liaisons are listed by state. The liaison will notify CI and other functions on their behalf. Advise the caller that they need to contact the liaisons as quickly as possible so the IRS can take steps to prevent the filing of fraudulent returns.
3. Advise the taxpayer they may want to contact the Federal Trade Commission or the Social Security Administration at:

Contact	Web Address	Contact Number
Federal Trade Commission (FTC)	www.ftc.gov/idtheft	877-438-4338
Social Security Administration (SSA)	www.ssa.gov search "Identity Theft"	800-772-1213

4. Advise the caller they may want to contact one of the major credit bureaus. They may be able to assist them in obtaining information needed to pursue issue relating to the loss of the businesses PII information.

Credit Bureau	Web Address	Contact Number
Equifax	equifax.com/business	800-525-6285
Experian	http://www.experian.com/business-services/business-services.html	888-397-3742
Transunion	http://www.transunion.com/business	800-680-7289

5. Advise the taxpayer they may want to file a report with their local or state police and contact their state Attorney General's office. Provide the web site information for a list of state Attorney General, <http://www.naag.org/>
6. Provide the taxpayer the [irs.gov](https://www.irs.gov) website advising them to search for "business identity theft", to obtain additional ID theft information.

25.23.11.6.2
(10-01-2023)

**Individual Taxpayers
Reporting to be Victims
of Business-Related
Identity Theft**

- (1) There will be times when a taxpayer contacts the Service advising they have no association with a business but have received a CP 575, Employer Identification Number (EIN) Assignment Notice confirming the assignment of an EIN. It is possible that an ID thief used someone's PII to obtain an EIN for a business.
- (2) If a Form 14039, Identity Theft Affidavit is received stating the taxpayer has no knowledge or association with the business, a referral must be sent to the BMF functional liaison. The BMF IDT SME's will send the Letter 5316C, BMF Identity Theft Documentation Acknowledgment Letter (Form 14039B and required documentation), if deemed a valid BMF IDT. If the contact is by phone, do not advise them to submit a Form 14039 or Form 14039-B, Business Identity Theft Affidavit.

Exception: The acknowledgement letter is not necessary if it is clear the case can be resolved within 30 days of receipt into BMF IDT inventory. Letter 5317C, BMF Identity Theft Request for Information or Closing Letter will serve as an acknowledgement. If work schedules do not allow for time to make this determination, or it is not clear then the 5316C should be sent to acknowledge receipt.

- (3) Research the IMF side to determine if there is any past association with the EIN. This will include schedule C, Schedule H or possible wages utilizing the EIN in question. See IRM 25.23.9.4.2, Individual Taxpayers Reporting to be Victims of Business Related Identity Theft, for additional information if needed.
- (4) If you are not trained in working ID theft, contact your team lead and refer to the appropriate BMF ID theft unit per IRM 25.23.11.6.4, BMF Identity Theft Paper Inquiry or IRM 25.23.11.6.5, BMF Identity Theft Phone Inquiry Made to a BMF AM CSR, using Form 14566, BMF Identity Theft Referral. For instruction on how to complete the form see Exhibit 25.23.11-1, Accounts Management Form 14566 Instructions.
- (5) If trained to work BMF ID theft cases and it is determined ID theft exists, research utilizing the *IAT BITR Tool* and CC IMFOLE, when BITR is unavailable, to determine if there is an existing TC 971 AC 504 MISC SPCL2. This marker on the IMF side identifies the association of BMF ID theft to the SSN owner. If there is currently no ID TC 971 AC 504 SPCL2 marker, the SSN entity must be marked on CC ENMOD using CC REQ77. Overlay the SSN ENMOD and complete the fields as follows:
 1. TC> 971
 2. Secondary Date> The related tax year
 3. TC 971/151-CD> 504
 4. XREF-TIN>EIN
 5. MISC>SPCL2
- (6) See IRM 25.23.2.8.1.2, TC 971 AC 504- Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFAIL, for additional information.

#####

- #####

- (6) If a TC 971 AC 711 posted suspending the return and a second return is filed that does not hit the filters, it will post as a TC 150. If a second return is filed and it also hits the filters, a second TC 973 will post to the account. There can be more than one TC 973 on the module.
- (7) The following table illustrates the codes and actions RICS will take based on the determination:

	If the selected return is determined to be:	And	Then:
1.	Not IDT	No questionable frivolous or fraudulent items are present	<p>RICS will take appropriate actions as follows:</p> <ul style="list-style-type: none"> Reverse the TC 971 AC 711 if present and input TC 971 AC 712 with corresponding DLN of the TC 973 to allow that return to post. If a TC 971 AC 522 is present, RICS will reverse as applicable.
2.	Not IDT	Frivolous items are present	<p>RICS will take appropriate actions as follows:</p> <ul style="list-style-type: none"> Refer the case to FRP for further review and will update activity to 'NOTIDT_FRP'. Reverse the TC 971 AC 711 if present and input TC 971 AC 713 with corresponding DLN of the TC 973 to allow that return to post and freeze any refund with a TC 810 (-Q freeze) RC 4. If a TC 971 AC 522 is present, RICS will reverse as applicable and notate case referred to other area for review.

	If the selected return is determined to be:	And	Then:
3.	Not IDT	Fraudulent items are present	<p>RICS will take appropriate actions as follows:</p> <ul style="list-style-type: none"> • Refer the case to SBSE for further review and will update activity to 'REF2SBSE'. • Reverse the TC 971 AC 711 if present and input TC 971 AC 717 with corresponding DLN of the TC 973 to allow that return to post and freeze any refund with a TC 810 (-Q freeze) RC 8. • If a TC 971 AC 522 is present, RICS will reverse as applicable and notate case referred to other area for review.
4.	Not IDT	the return was deleted from the suspense file	<p>RICS will take appropriate actions as follows:</p> <ul style="list-style-type: none"> • Reverse the TC 971 AC 711 • Send the return for processing using the original received date. <p>Reminder: The original DLN will be crossed out on the return for processing to assign a new DLN.</p>

	If the selected return is determined to be:	And	Then:
5.	IDT or Fabricated EIN		<p>RICS will post a TC 971 AC 522 CLSIDT, and/or document AMS notes with the determination.</p> <p>If EIN is deemed fabricated, RICs will also:</p> <ul style="list-style-type: none"> • Update the entity with "POTENTIAL FAB EIN" on the sort name line. • Input on CC ENMOD a TC 971 AC 524 containing EINFAB in the MISC field to lock the EIN. <p>Reminder: If the EIN is deemed fabricated, BMF AM not specialized in IDT casework, should not make any adjustments on the account. Refer to specific guidance in IRM 21.7.2.4.6.13, Forms 94XX with Return Integrity and Compliance Services (RICS), Return Integrity Verification Operations (RIVO), or Identity Theft (IDT) Involvement, for referral to BMF IDT.</p>

#

	If	Then
1.	<p>There is an unreversed TC 971 AC 524 input on ENMOD or BMFOLE containing EINFAB or EINFB2 in the MISC field</p> <p>Note: TC 971 AC 524 containing EINFAB in the MISC field deemed fabricated by RICS will include 'POTENTIAL FAB EIN' in the sort name line. TC 971 AC 524 containing EINFB2 deemed fabricated by RICS may or may not include 'POTENTIAL FAB EIN' in the sort name line.</p>	<ul style="list-style-type: none"> • Include in the subject line of the secure email 'BTA Access Reconsideration' and the last 4 digits of the EIN (i.e., 'BTA Access Reconsideration 8765'). • Advise the taxpayer their account will need to be referred to another area for review and the timeframe for review is up to 60 days. <p>After the 60 day timeframe has passed, continue to follow the instructions above every 60 days (as needed) if the taxpayer does not receive a response.</p> <ul style="list-style-type: none"> • Include in the subject line of the secure email 'BTA Access Reconsideration: X Request', where 'X' is the request number (i.e., second, third, etc.), and the last 4 digits of the EIN (i.e., 'BTA Access Reconsideration: Second Request 8765'). • Advise the taxpayer their account will need to be referred to another area for review and the timeframe for review is up to 60 days.

#

	If	Then
2.	<p>There is an unreversed TC 971 AC 524 input on ENMOD or BMFOLE containing EINFAB or EINFB2 in the MISC field and 'Identity Theft' is present in the sort name line</p> <p>Note: AM BMF Identity Theft always includes 'Identity Theft' in the sort name line when deeming an account fabricated.</p>	<ul style="list-style-type: none"> • Send a Form 14566, BMF Identity Theft Referral, by secure email to the AM BMF IDT liaison at <i>*TS AM BMF IDT</i>. In the referral, explain the taxpayer is attempting to access BTA and/or ECO and the account needs reconsideration. • Include in the subject line of the secure email 'BTA Access Reconsideration' and the last 4 digits of the EIN (i.e., 'BTA Access Reconsideration 8765'). • Advise the taxpayer their account will need to be referred to another area for review and the timeframe for review is up to 120 days. • Correspondence will be sent to the taxpayer to let them know the results of the review.

- (9) If the taxpayer **calls** and the original return is being held for RICS review, or the return is pending RICS review, follow the If/Then chart below:

	If the taxpayer calls and	Then
1.	The taxpayer states they did not receive a Letter 6042C and RICS has not made a final determination of ID theft	<p>1. Send an e4442 referral to</p> <p>Section B of the e4442, request RICS re-issue the letter and include additional information the taxpayer provides</p> <p>Note: If the taxpayer states their address has changed, do not update the address on the account. Notate the address change on the referral and advise the taxpayer to submit Form 8822-B. Refer to IRM 21.1.3.20.1, IMF and BMF Oral Statement Address Changes for additional information.</p> <p>2. Explain to the taxpayer their tax return is under review and they must respond to the letter providing the requested information.</p> <p>3. Advise the taxpayer they should receive the reissued letter within 30 days.</p> <p>Reminder: Do not reissue the letter to the taxpayer. Only RICS can reissue the letter.</p>

#

	If the taxpayer calls and	Then
2.	<p>The taxpayer states they did not receive a Letter 6042C and RICS has made a final determination of ID theft. For example, research may show any of the following (this is not all-inclusive):</p> <ul style="list-style-type: none"> • Closed RICS control with IDRS activity code of IDTCON-FRMD • An unreversed TC 971 AC 522 containing CLSIDT posted to tax module • A previous request to reissue the letter and AMS/IDRS history indicates RICS has made a final IDT determination, and the letter will not be reissued <p>Note: RICS does not send determination letters for Entity Fabrication (EF) or ID theft programs. If RICS has made a determination of ID theft, they do not communicate with or respond back to the individual. Refer to actions taken on AMS/IDRS to see the case determination made by RICS.</p>	<ol style="list-style-type: none"> 1. Advise the taxpayer after review of their account, the return was determined to be an invalid filing. The return will not be processed, and a refund will not be issued or overpayments applied. 2. Advise the taxpayer if they have additional information to support the return filed, please fax that supporting documentation to 844-201-5531.

	If the taxpayer calls and	Then
3.	Claims they have no knowledge of the business referenced on the notice/ letter	<div><div>1.</div><div>Advise the taxpayer to submit a signed statement with a copy of their Letter 6042C via fax or to the address provided on the letter.</div><div>2.</div><div>Advise the taxpayer it can take up to 9 weeks to review and complete account actions from the received date of their letter response.</div></div>
4.	Questions the notice/letter or is asking for assistance	<div><div>1.</div><div>Advise the taxpayer they must reply to the Letter 6042C and provide the requested information via fax or to the address provided on the letter.</div><div>2.</div><div>Advise the taxpayer it can take up to 9 weeks to review and complete account actions from the received date of their letter response.</div></div>

#

	If the taxpayer calls and	Then
5.	<p>If the taxpayer responded to the Letter 6042C , Entity Verification for Businesses, and calls back claiming they did not receive a refund or their return did not complete processing due to RICS review, no confirmed BMF IDT TC posted to the account and 9 weeks have passed from the taxpayer's letter response received date</p> <p>Note: If 9 weeks have not passed from the date the taxpayer's response was received, advise the taxpayer it can take up to 9 weeks to review.</p>	<p>1. Send an e-4442 using</p> <p>Note: If the taxpayer states their address has changed, do not update the address on the account. Notate the address change on the referral and advise the taxpayer to submit Form 8822-B. Refer to IRM 21.1.3.20.1, IMF and BMF Oral Statement Address Changes for additional information.</p> <p>2. Advise the taxpayer actions will be completed within 30 days.</p>
6.	<p>If the taxpayer responded to Letter 6042C and did not receive a refund or their return did not process due to RICS review, and a confirmed BMF IDT transaction code posted to the account</p> <p>Note: RICS does not send determination letters for Entity Fabrication (EF) or ID theft programs. If RICS has made a determination of ID theft, they do not communicate with or respond back to the individual. Refer to actions taken on AMS/IDRS to see the case determination made by RICS.</p>	<p>1. Advise the taxpayer after review of the response to letter 6042C, the return was determined to be an invalid filing. The return will not be processed, and a refund will not be issued or overpayments applied.</p> <p>2. Advise the taxpayer if they have additional information to support the return filed, please fax that supporting documentation to 844-201-5531.</p>

#

	If the taxpayer calls and	Then
7.	<p>The taxpayer submitted additional information to support the return filed and states they did not receive a refund or their return was determined to be an invalid filing due to RICS review, and 9 weeks have passed from the taxpayer's response received date with no update to the IDT determination. For example, research may show any of the following (this is not all-inclusive):</p> <ul style="list-style-type: none"> • Closed RICS control with IDRS activity code of NOTIDT • TC 971 AC 522 containing CLSIDT reversed with TC 972 AC 522 containing NOTIDT posted to the tax module • TC 971 AC 711 reversed with TC 971 AC 712, TC 971 AC 713, or TC 971 AC 717 with corresponding DLN on TC 973 to allow the return to post • AMS narrative indicating no IDT and actions taken <p>Note: If 9 weeks have not passed from the date the taxpayer's response was received, advise the taxpayer it can take up to 9 weeks to review.</p>	<p>1. Send an e-4442 using</p> <p>Note: If the taxpayer states their address has changed, do not update the address on the account. Notate the address change on the referral and advise the taxpayer to submit Form 8822-B. Refer to IRM 21.1.3.20.1, IMF and BMF Oral Statement Address Changes for additional information.</p> <p>2. Advise the taxpayer actions will be completed within 30 days.</p>

#

	If the taxpayer calls and	Then
8.	<p>If the taxpayer submitted additional information to support the return filed and states they did not receive a refund or their return was determined to be an invalid filing due to RICS review, and RICS has confirmed the final determination of ID theft</p> <p>Note: RICS does not send determination letters for Entity Fabrication (EF) or ID theft programs. If RICS has made a determination of ID theft, they do not communicate with or respond back to the individual. Refer to actions taken on AMS/IDRS to see the case determination made by RICS.</p>	<p>1. Advise the taxpayer after review of the additional information submitted, the return was determined to be an invalid filing. The return will not be processed, and a refund will not be issued or overpayments applied.</p> <p>2. Advise the taxpayer if they have additional information to support the return filed, please fax that supporting documentation to 844-201-5531.</p>

Note: The taxpayer does NOT need to file a Form 14039 or Form 14039-B; RICS will ensure all appropriate actions to protect the taxpayer's account will be taken.

- (10) If a **paper** case is received that meets the criteria mentioned above, follow the chart below:

	If the case is	The tax module may show	Then
1.	A response to Letter 6042C, Entity Verification for Businesses		<p>Forward the case to RICS Unit, Ogden Service Center, Stop 9002 OR fax the response to 844-201-5531.</p> <p>Note: The fax number is only to be used for responses to Letter 6042C.</p>

	If the case is	The tax module may show	Then
2.	A response to a CP notice requesting a return to be filed (e.g., CP 80 or CP 259) but original return is being held pending RICS review		Forward the case to RICS Unit, Ogden Service Center, Stop 9002 Note: Responses to CP notices must be routed to Stop 9002. There is no other method of delivery available.
3.	A duplicate/amended return but there is no posted TC 150 because the original return is being held pending RICS review and it has been 23 weeks since RICS selected the original return (TC 973) Note: The 23 weeks is figured from the TC 973 posted cycle. See <i>SERP - 6209 - IRM Supplements (irs.gov)</i> , and select Section 16, Julian Date, Cycle and Notice Calendars. Select the applicable TIF Processing Cycles chart to determine if the timeframe has been met.	<ul style="list-style-type: none"> • TC 971 AC 711 • TC 973 • Open control assigned to 1481055555 • IDRS activity code POTENTIDT 	Send a referral (e-4442 or fax if e-4442 is not available) using to RICS requesting RICS review the case for a determination. Upon RICS determination, continue processing per the applicable scenarios below.

#

	If the case is	The tax module may show	Then
4.	<p>A duplicate/amended return but there is no posted TC 150 because the original return is being held pending RICS review and it has not been 23 weeks since RICS selected the original return (TC 973)</p> <p>Note: The 23 weeks is figured from the TC 973 posted cycle. See <i>SERP - 6209 - IRM Supplements (irs.gov)</i>, and select Section 16, Julian Date, Cycle and Notice Calendars. Select the applicable TIF Processing Cycles chart to determine if the timeframe has been met.</p>	<ul style="list-style-type: none"> • TC 971 AC 711 • TC 973 • Open control assigned to 1481055555 • IDRS activity code POTENTIDT 	<p>Suspend the case and monitor for RICS to make a determination.</p> <p>If the 23 week timeframe passes with no determination from RICS, send a referral as indicated in Box 3 above.</p> <p>Upon RICS determination, continue processing per the applicable scenarios below.</p> <p>Exception: You must continue to monitor for a RICS determination. If there is any indication the TP responded to Letter 6042C (example: AMS history shows taxpayer responded and no 4442 has been sent, or RICS IDRS control activity shows a response received) and it has been 9 weeks since the TP response was received by RICS, send an e-4442 to RICS requesting they review the case for a determination.</p>

	If the case is	The tax module may show	Then
5.	A duplicate/amended return, there is a TC 150 posted, RICS determination is Not IDT and the return was not referred to another area for review of questionable frivolous or fraudulent items claimed on the return.	<ul style="list-style-type: none"> • TC 971 AC 712 with corresponding DLN of the TC 973 to allow the return to post • RICS IDRS control is closed • IDRS activity code indicates NOTIDT 	<p>Do not refer to BMF IDT and process using normal procedures as found in IRM 21.7.9 , BMF Duplicate Filing Conditions.</p> <p>Reminder: Follow IRM procedures for any applicable freeze codes on the module. There may be instances where a freeze code should not be released.</p>
6.	A duplicate/amended return, there is a TC 150 posted, RICS determination is Not IDT and the return was referred to another area for review of questionable frivolous or fraudulent items claimed on the return.	<ul style="list-style-type: none"> • TC 971 AC 713 or AC 717 with corresponding DLN of the TC 973 to allow the return to post • RICS IDRS control is closed • Refund frozen with a TC 810 (-Q freeze) • AMS/IDRS history notes will indicate the return is not IDT and referred to other area for review. 	<p>Do not refer to BMF IDT and process using normal procedures as found in IRM 21.7.9 , BMF Duplicate Filing Conditions.</p> <p>Reminder: Follow IRM procedures for applicable freeze codes on the module (i.e., -Q) and the control base histories. There will be instances where a freeze code should not be released.</p>

	If the case is	The tax module may show	Then
7.	A duplicate/amended return and RICS determination is IDT or a Fabricated EIN determination has been made	<ul style="list-style-type: none"> Unreversed TC 971 AC 522 MISC CLSIDT and/or AMS/IDRS indicates IDT determination 'POTENTIAL FAB EIN' on the sort name line if the EIN is determined to be fabricated Unreversed TC 971 AC 524 input on ENMOD containing EINFAB in the MISC field 	<p>Prepare Form 14566, BMF Identity Theft Referral, and send by secure email to the AM BMF IDT liaison at <i>*TS AM BMF IDT</i>. In the subject line of the secure email, include the tax year of the case that is being referred.</p> <p>Note: If the BMF case involves a CARES Act COVID-19 related credit, include in subject line of the secure email the specific COVID related credit, as well as the tax year of the case (i.e., 'Sick and Family Leave 202103 - Form 14566,' or 'ERC 202103 - Form 14566').</p> <p>Note: If the BMF case includes CI involvement (-Z freeze, etc.), the referral must include the account has CI involvement.</p> <p>The account will be reviewed to confirm the original determination is still valid.</p>
8.	Any other case type (penalty abatement, correspondence, etc.)		Advise the taxpayer Letter 6042C has been issued and they need to respond to the letter.

25.23.11.6.3.1
(10-01-2024)
**BMF Accounts with
RICS and/or IDT
Involvement - AM BMF
Identity Theft Teams
Only**

- (1) This subsection provides guidance for AM BMF IDT SMEs when a claim is received and there is ID theft or RICS involvement on the tax module or account.
- (2) AM BMF employees will submit referrals to the AM BMF IDT Liaison when claims are received and there is IDT, or the EIN has been determined to be fabricated. The cases will be assigned to the AM BMF IDT SMEs for resolution.

Note: RICS initial determination does not need confirmation from RICS unless the taxpayer provides additional information, or the SME identifies additional information that RICS did not take into consideration. If a referral must be sent to RICS, send Form 14566, BMF Identity Theft Referral, via secure email to

the AM BMF IDT Liaison. The referral must include the reason for RICS to reconsider their initial determination and all supporting documentation provided by the taxpayer, if applicable.

- (3) Form 14039, Identity Theft Affidavit/Form 14039-B, Business Identity Theft Affidavit, may also be received from the taxpayer claiming ID theft.
- (4) Follow the chart below to resolve BMF accounts with RICS and/or IDT involvement:

	If account shows	And	Then
1.	E- Freeze (TC 150 is not posted, and account shows RICS involvement)	Closed RIVO control, TC 971 AC 711, or TC 973 on module, AMS/IDRS indicates IDT determination made or unreversed TC 971 AC 522 (MISC CLSIDT) is present on the module or Sort name line includes 'POTENTIAL FAB EIN,' and TC 971 AC 524 is present on the module	<p>Do not process the amended/duplicate return.</p> <p>Send the taxpayer Letter 916C, Claim Incomplete for Processing; No Consideration, to the address of record.</p> <p>If the sort name line includes "Potential Fab EIN," remove it from the letter prior to transmitting. (Do not update the sort name line on the account.)</p> <p>Do NOT update the address of record if it differs from the address on the amended/duplicate return.</p> <p>Include the following language when sending the letter to the taxpayer:</p> <p><i>Your original return was determined to be an invalid filing. Your amended return will not be processed, and a refund will not be issued, or overpayments applied. If you have any additional information to support the return filed, please fax supporting documentation to 844-201-5531.</i></p> <p>Input TC 971 AC 002 to release the E- freeze.</p>

	If account shows	And	Then
2.	-A Freeze (TC 150 is posted) and a Fabricated EIN determination has been made by RICS	AMS/IDRS indicates a Fabricated EIN determination was made Sort name line includes 'POTENTIAL FAB EIN,' and TC 971 AC 524 is present on the module	Do not process the amended/duplicate return. Send the taxpayer Letter 916C, Claim Incomplete for Processing; No Consideration, to the address of record. Do NOT update the address of record if it differs from the address on the amended/duplicate return. If the sort name line includes "Potential Fab EIN," remove it from the letter prior to transmitting. (Do not update the sort name line on the account.) Include the following language when sending the letter to the taxpayer: <i>Your original return was determined to be an invalid filing. Your amended return will not be processed, and a refund will not be issued, or overpayments applied. If you have any additional information to support the return filed, please fax supporting documentation to 844-201-5531.</i> Input TC 290 for .00 to release the -A freeze, if applicable.

	If account shows	And	Then
3.	-A Freeze (TC 150 is posted) and a prior Fabricated EIN determination was made by AM BMF IDT	AMS/IDRS indicates a Fabricated EIN determination was made Sort name line includes 'IDENTITY THEFT,' and TC 971 AC 524 is present on the module	Do not process the amended/duplicate return. Send the taxpayer Letter 916C, Claim Incomplete for Processing; No Consideration, to the address of record. If the sort name line includes "Identity Theft," remove it from the letter prior to transmitting. (Do not update the sort name line on the account.) Do NOT update the address of record if it differs from the address on the amended/duplicate return. Include the following language when sending the letter to the taxpayer: <i>Your original return was determined to be an invalid filing. Your amended return will not be processed, and a refund will not be issued, or overpayments applied. If you have additional information to verify the above EIN is valid, please submit the documentation with a copy of this letter.</i> Input TC 290 for .00 to release the -A freeze, if applicable.

	If account shows	And	Then
4.	<p>-A Freeze (TC 150 is posted) and an IDT determination has been made by RICS. The account has not been deemed fabricated and is not locked. Research must be conducted to determine if the TC 150 that is posted to the account is the taxpayer's valid return. For example (this list is not all-inclusive):</p> <ul style="list-style-type: none"> • The return was submitted by the taxpayer • A return was not sent for processing in error (research CII for prior cases, etc.) 	<p>AMS/IDRS indicates IDT determination made or unreversed TC 971 AC 522 (MISC CLSIDT) is present on the module and TC 971 AC 711 MISC field does not match the TC 150 DLN</p>	<p>Reject the referral back to the originator and advise them the identity theft issue has been resolved and the TC 150 appears to be valid. They can follow normal procedures to process the amended/duplicate return.</p>

	If account shows	And	Then
5.	<p>-A Freeze (TC 150 is posted) and an IDT determination has been made by RICS. The account has not been deemed fabricated and is not locked. Research must be conducted to determine if the TC 150 that is posted to the account is the taxpayer's valid return. For example (this list is not all-inclusive):</p> <ul style="list-style-type: none"> • The return was submitted by the taxpayer • A return was not sent for processing in error (research CII for prior cases, etc.) 	<p>AMS/IDRS indicates IDT determination made or unreversed TC 971 AC 522 (MISC CLSIDT) is present on the module and TC 971 AC 711 MISC field does not match the TC 150 DLN and You determine the TC 150 return is not the taxpayer's valid return</p>	<p>Do not process the amended/duplicate return. Send the taxpayer Letter 916C, Claim Incomplete for Processing; No Consideration, to the address of record. Do NOT update the address of record if it differs from the address on the amended/duplicate return. Include the following language when sending the letter to the taxpayer: Your original return was determined to be an invalid filing. Your amended return will not be processed, and a refund will not be issued, or overpayments applied. If you have any additional information to support the return filed, please fax supporting documentation to 844-201-5531. Input TC 290 for .00 to release the -A freeze, if applicable.</p>

	If account shows	And	Then
6.	Form 14039/Form 14039-B is submitted by the taxpayer claiming ID theft		Resolve the taxpayer's claim of ID theft following normal ID theft procedures. Send the taxpayer Letter 5317C, BMF Identity Theft Request for Information or Closing Letter.

#

	If	And	Then
1.	The account indicates RICS deemed the account fabricated	There is an unreversed TC 971 AC 524 input on ENMOD or BMFOLE containing EINFAB or EINF2 in the MISC field and 'Potential Fab EIN' is present in the sort name line	Return the referral to the originator and advise them to send a Form 4442 to RICS per IRM 25.23.11.6.3 , BMF Returns Selected for RICS Review, so that RICS can reconsider the determination.

2.	The account indicates AM BMF IDT deemed the account fabricated	There is an unreversed TC 971 AC 524 input on ENMOD or BMFOLE containing EINFAB or EINF2 in the MISC field and 'Identity Theft' is present in the sort name line	<p>Perform all research detailed in IRM 25.23.9.4, BMF Identity Theft Research, and Exhibit 25.23.9-7, BMF Identity Theft Research Requirement, to reconsider the validity of the EIN.</p> <p>Reminder: Check AMS, CII, etc. for prior TP inquiries reporting they did not request the EIN or stated they had identity theft on the EIN (phone calls, CII cases, etc.).</p> <p>1. If, through research, you determine the EIN is not fabricated and the account should be unlocked:</p> <ul style="list-style-type: none"> • Document your findings on Form 14566, BMF Identity Theft Referral • Include all appropriate research completed on the referral and explain why the account needs to be unlocked. • On the subject line of the referral, enter: TC 972 AC 524 BTA Access and CII Case ID if applicable. • Research CII for the original case and, if available, attach the PDF print of the original entity (CC ENMOD) to the secure e-mail. If the original case does not have a PDF print of the original entity attached, notate in the referral that the information was not available.
----	--	--	---

			<ul style="list-style-type: none">• Send the completed referral to your AM BMF Identity Theft liaison by secure e-mail using the *TS AM BMF IDT, referral to IP, Entity Fabrication (EF) Team in RICS, and CI.• Document the sending of the referral on AMS along with the details of the request. If working a CII case, attach the referral to the case.• Once IP confirms the account has been unlocked, monitor the case until the TC 012 and TC 972 AC 524 are posted.• Update the entity to remove 'Identity Theft' from the sort name line.• If the account is a sole proprietorship, input the sole proprietor link to the cross-reference SSN.
--	--	--	---

			<ul style="list-style-type: none">• Send the taxpayer Letter 5317C using an open paragraph with the following language: <i>After review of your account, we unlocked this employer identification number (EIN). Access to Business Tax Account is now available.</i> Note: If the EIN is for a sole proprietorship, also include the following language: <i>We restored all references to your name and Social Security number (SSN) in association with this employer identification number.</i> <p>2. If, through research, you determine the EIN is fabricated and the account should remain locked:</p>
--	--	--	---

			<ul style="list-style-type: none"> Send the taxpayer Letter 5317C and include the following verbiage in two open paragraphs: <i>After review of your account, we have determined the above employer identification number (EIN) should remain locked at this time. If you have additional information to verify the above EIN is valid, please submit the documentation with a copy of this letter. If a Sole Proprietor, provide two of the following: valid U.S. Federal or State government issued identification with your signature, and documentation to support your business operation (i.e., utility bill or invoice). If a Partnership or Limited Liability Company, provide one or more of the following: articles of incorporation, articles of organization, or other supporting documentation.</i>
--	--	--	--

25.23.11.6.4
(05-14-2024)

BMF Identity Theft Paper Inquiry

- (1) The taxpayer may submit a paper inquiry after receiving an unexpected notice regarding an inactive or active employer identification number (EIN), a recently-established EIN they have no knowledge about, or a balance due notice for a BMF form they never filed with IRS. Since the contact is unexpected, the taxpayer's correspondence may indicate they are a victim of business identity theft (BMF IDT).

Note: If there is an unreversed TC 971 AC 522 already on the module and/or an open ID theft control, see IRM 25.23.11.6 (2), BMF Identity Theft Inquiries, to determine if the case needs to be referred. If the case needs to be referred see IRM 25.23.11.6.6, BMF Identity Theft Referrals - AM BMF Identity Theft Teams Only, for referral procedures.

- (2) After research has been performed to rule out potential mixed entity/period or other account situations, and there is potential identity theft, non-specialized IDT teams follow the chart below:

Step	Action
1	Review the table under IRM 25.23.11.6, BMF Identity Theft Inquiries, to determine if the account needs to be placed in another function's BMF IDT inventory. If the table indicates a referral is necessary, take the following action:
2	Do not reassign or close the control base.
3	Do not input a TC 971 AC 522. The receiving function will input the ID theft indicator after the referral is accepted in their inventory.
4	Initiate the Form 14566, BMF Identity Theft Referral. See Exhibit 25.23.11-1, Accounts Management Form 14566 Instructions.
5	<p>After review by a lead, send the Form 14566 by secure e-mail to the applicable liaison per IRM 25.23.11.6, BMF Identity Theft Inquiries. If Form 14039 or Form 14039-B is present, attach the form to the secure e-mail when referring the case. In the subject line of the secure e-mail, include the tax year of the case that is being referred.</p> <p>a. If the case requires referral to BMF AM IDT inventory, send the Form 14566, BMF Identity Theft Referral, by secure e-mail to the appropriate site per your location:</p> <p>b. If the case requires referral to another function's BMF IDT inventory, send the Form 14566, BMF Identity Theft Referral by secure e-mail to <i>*TS AM BMF IDT</i>.</p>
6	<p>Update the CII History Notes to show: Potential BMF IDT - Case referral to [insert the function's name].</p> <p>Example: Potential BMF IDT - Case referral to Field Collection</p>
7	Once the case is accepted by the referring function, close the control.

#

Reminder: If there is a balance due on the account relating to the ID theft issue, input a TC 470.

- (3) If the case is to remain in AM IDT inventory, SMEs will take the following steps:

Step	Action
1	If a control is not open, open the control
2	If the taxpayer sent the Form 14039 or 14039-B, send Letter 5316C, to acknowledge claim receipt. Exception: The acknowledgement letter is not necessary if it is clear the case can be resolved within 30 days of receipt into BMF IDT inventory. Letter 5317C, BMF Identity Theft Request for Information or Closing Letter will serve as an acknowledgement. If work schedules do not allow for time to make this determination, or it is not clear then the 5316C should be sent to acknowledge receipt.
3	Input TC 971 AC 522 IDTCLM on all MFTs and tax periods involved in the ID theft when the taxpayer claims ID theft but no documentation is sent.
4	Input the TC 971 AC 522 IDTDOC if the Form 14039 or 14039-B is received. If there is no previous TC 971 AC 522 IDTCLM present and a Form 14039/14039-B received, just input the TC 971 AC 522 IDTDOC
5	Update CII notes providing facts behind ID theft determination.
6	Once the research is completed and ID theft is established, the case must be reviewed by Manager or Lead, prior to taking any account actions. Follow local procedures for the review process.
7	Once the review process is completed and ID theft is well established, see IRM 25.23.11.6.7, Account Actions - AM BMF Identity Theft Teams Only, for steps to correct the account.
8	Review the account to determine if there are any other outstanding issues that need to be addressed. (For example, collection issues, defaulted installment agreement, offsets or missing returns.) (This list is not all inclusive.)
9	Once account has been corrected and all issues addressed send Letter 5317C, BMF Identity Theft Interim & Post Resolution Letter and input TC 971 AC 522 CLSIDT.

Note: Paragraphs 4-5 below are for BMF IDT SMEs only

- (4) If ID theft cannot be established through internal research and additional information is needed, send the taxpayer Form 14039-B, Business Identity Theft Affidavit using Letter 5317C, BMF Identity Theft Interim & Post Resolution Letter. See IRM 25.23.9.7, Form 14039-B, Business Identity Theft Affidavit, for additional information. Give the taxpayer 30 days to respond to the notice. Suspend the case for 45 days to allow the taxpayer time to respond.

- a. If a response has not been received within that time frame, close the case and reverse the ID theft indicator with TC 972 AC 522 NORPLY. Reverse the TC 470 if one was placed on the account. Send Letter 5317C, BMF Identity Theft Interim & Post Resolution Letter, using the appropriate paragraphs.
- b. If the taxpayer provides the needed information review it for completeness, legibility and determine whether all required information has been included. If the claim is complete, input a TC 971 AC 522 IDTDOC to indicate receipt of the Form 14039-B and send the Letter 5316C to acknowledge receipt of the claim and take all necessary account actions to resolve the ID theft issue. See IRM 25.23.11.6.7, Account Actions, for the steps to correct the account.

Exception: The acknowledgement letter is not necessary if it is clear the case can be resolved within 30 days of receipt into BMF IDT inventory. Letter 5317C, BMF Identity Theft Request for Information or Closing Letter will serve as an acknowledgement. If work schedules do not allow for time to make this determination, or it is not clear then the 5316C should be sent to acknowledge receipt.

- c. If there are missing documents, attempt to call the taxpayer if there is a contact number provided. Document the CII case notes with dates, times of the calls, the name of the contact and what information was requested from the taxpayer. If phone contact cannot be made within three business days or no number is provided, issue a Letter 5317C to the taxpayer requesting the needed information. In both cases, provide a 30-day time frame for submission of any missing information. If the follow-up response is not received within the 45 days, follow the procedures in (a) to close the case.
 - d. If, after receipt of the 14039-B, ID theft still cannot be established, send Letter 5317C using the appropriate paragraphs to provide taxpayer a complete explanation as to why the Non-IDT determination was made.
- (5) If a Form 14566 is received and the case is not on CII, follow normal procedures for sending the case to be scanned with the activity code **BMF IDT** and appropriate category code: BID1-Employment Tax, BID2-Form 1120 or BID3-Other. Once the case is scanned into CII, send Letter 5316C if not already sent and input TC 971 AC 522 IDTCLM if not already on the module(s), then follow the procedures stated above.

Exception: The acknowledgement letter is not necessary if it is clear the case can be resolved within 30 days of receipt into BMF IDT inventory. Letter 5317C, BMF Identity Theft Request for Information or Closing Letter will serve as an acknowledgement. If work schedules do not allow for time to make this determination, or it is not clear then the 5316C should be sent to acknowledge receipt.

25.23.11.6.5
(10-01-2024)
**BMF Identity Theft
Phone Inquiry Made to a
BMF AM CSR**

- (1) The taxpayer may contact a BMF phone application claiming to be a victim of business identity theft (BMF IDT) when they suspect the name and EIN of their business entity, estate, trust, or exempt organization was used without consent to file tax returns or income documents. Other common reasons for taxpayer contact include the following (this list is not all-inclusive):

- Receiving an unexpected notice regarding an inactive EIN
- Receiving a balance due notice for a BMF form they never filed with the IRS
- Receiving a rejection notice for an electronically filed return because the IRS already has a return on file for that same tax period and MFT
- The taxpayer/caller never applied for an EIN but is receiving notices for a business in their name. Send Form 14566, BMF Identity Theft Referral, to the appropriate BMF ID theft unit. See IRM 25.23.11.6.2, Individual Taxpayers Reporting to be Victims of Business-Related Identity Theft, for additional information.
- The business, estate, trust or exempt organization experienced a data breach with no tax-related impact to the business entity. For example, a business reports a breach of their computer system and after thorough research of the account, there is no evidence of a fraudulent tax return or income documents being filed. If the taxpayer/caller is seeking advice about the data breach of their business entity, ask the taxpayer/caller about the type of information that was breached. See IRM 25.23.11.6.1, Non-Tax Related Identity Theft, for additional information.

- (2) Follow the normal telephone and authentication requirements under IRM 21.1.1.4, Communication Skills, and IRM 21.1.3.2.3(6), Required Taxpayer Authentication.

Caution: If there is an ID theft indicator on the module, high risk disclosure authentication must be completed to ensure you are speaking to an authorized party. Refer to IRM 21.1.3.2.4, Additional Taxpayer Authentication.

Note: When the caller claims to be an identity theft victim and is unable to pass disclosure authentication, we will accept the taxpayer's statement and not provide any account information. Update the history with the caller's contact information and a brief explanation of the potential identity theft. The documentation must include the statement: **Potential BMF IDT; caller unable to pass disclosure**. Proceed with the required research to determine ID theft potential. If the taxpayer states they have no knowledge of the business, they may be unable to pass BMF disclosure. Utilize the information under the caller's TIN to verify identity prior to disclosing any information.

Reminder: IMF disclosures requirements are:

1. SSN/ITIN
2. Name(s) as they appear on the last return filed
3. Current address
4. DOB
5. For additional information see IRM 21.1.3.2.3, Required Taxpayer Authentication. If taxpayer cannot answer these questions, see IRM 21.1.3.2.4, Additional Taxpayer Authentication.

- (3) When the caller indicates no knowledge of the EIN or business account, there are several reasons a third party may have requested an EIN on the taxpayer's behalf for a legitimate business purpose. You **must** expand the normal probe questions to determine if the EIN is legitimate or if there is a high probability of identity theft. Ask the caller the following questions:

- Did a family member take over a previously-owned business and request an EIN in your name or continue to use an inactive EIN assigned to you several years ago?
- Did you join a partnership or participate in the creation of a company where you provided your taxpayer identification number (TIN)?
- Did you provide your TIN to a community association or accountant to prepare tax returns on your behalf or a third party?
- Did you create a trust or other fiscal entity through a bank or executor?
- Have you received any home care services while enrolled in a program administered by a Federal, state, or local government agency that provides funding for the home care services? If yes, a 3rd party Agent may be authorized to act on behalf of the home care recipient to report and pay Federal employment taxes which requires an EIN.

Note: This list is not all inclusive and additional probes can be found at IRM 25.23.9.4(3), BMF Identity Theft Research.

- (4) Complete all initial research to rule out normal account issues and determine if the potential for ID theft exists. See IRM 25.23.11.4, Business Master File (BMF) ID Theft Research, for additional information.

Note: If an account related issue has created the problem and no ID theft exists, follow normal procedures to resolve the problem.

- (5) If the required research has been completed, and **additional information is still needed to determine if ID theft exists**, only request the taxpayer complete Form 14039-B, Business Identity Theft Affidavit, if the case is going to remain within AM for resolution. Form 14039-B can be found at [IRS.gov](https://www.irs.gov). Advise the taxpayer they need to return the Form 14039-B within 30 days. If there is a balance due on the account and additional information is needed, input a 6 cycle STAUP to provide the taxpayer time to send in the information. Do not open a control. A control will be opened in CII, Correspondence Imaging Inventory, when the taxpayer submits the requested information. If the taxpayer requests assistance completing Form 14039-B, see IRM 25.23.11.6.5.1, CSR Telephone Guidance for Form 14039-B, for additional information.
- (6) Once it has been determined identity theft exists, refer to IRM 25.23.11.6, BMF Identity Theft Inquiries, to assist with determining if the inquiry should be transferred or remain in AM.
- (7) Update AMS with the information that supports the ID theft determination or request for additional information.
- (8) If the inquiry is going to be referred to another function:

Step	Action
1	Complete Form 14566, BMF Identity Theft Referral, and forward the case to the team leadership for case review and approval to refer. Once the referral is approved, refer to IRM 25.23.11.6, Business Master File (BMF) Identity Theft Inquiries, for additional referral information.

Step	Action
2	Do not input a TC 971 AC 522. The function that will be resolving the ID theft issue will input the indicator and open the control.
3	If it is determined there is potential ID theft on an account with a balance due, input a TC 470 on all involved modules, if appropriate, to prevent the account from moving through the collection stream.
4	<p>Advise the taxpayer that due to the complexity of ID theft, their case will need to be referred to the ID theft area and to allow 120 days for resolution. Advise the taxpayer a hold has been placed if there was a balance owed relating to the ID theft issue.</p> <p>Note: If the balance due is the taxpayer's true liability or there are other outstanding account issues, follow normal procedures after handling the ID theft issue.</p>

- (9) If, after research, a potential for ID theft is determined and the case will remain in the BMF AM inventory:

Step	Action
1	Complete a Form 14566. Forward the referral to the appropriate site via secure e-mail advising the case needs to be scanned into CII and moved into the BMF ID Theft inventory. In the subject line of the secure e-mail, include the tax year of the case that is being referred. The contacts for the sites are:
2	<p>Input TC 971 AC 522 IDTCLM with the Secondary date being the date of the call.</p> <p>Exception: Input one day prior to the date of the call if today's date does not work.</p> <p>See IRM 25.23.9-2, BMF ID Theft Indicators- TC 971 AC 522 IDTCLM-Initial Allegation or Suspicion of BMF ID Theft, for additional information. In the MISC field enter WI AM IDTCLM, see IRM 25.23.9-1, TC 971 AC 5XX-MISC Codes, for additional information.</p>
3	Open the control with activity code "BMFIDT-REF" and the appropriate category code: BID1-Employment Tax, BID2-Form 1120 or BID3-Other. The case will be recontrolled once it is received into AM BMF IDT inventory.

#

25.23.11.6.5.1
(10-01-2024)
**CSR Telephone
Guidance for Form
14039-B**

- (1) After completing all initial research to rule out normal account issues, and additional information is still needed to determine if ID theft exists, the taxpayer should complete Form 14039-B if the case is going to remain in AM for resolution.
- (2) Form 14039-B can be found on [irs.gov](https://www.irs.gov). If the taxpayer requests assistance completing Form 14039-B, see the guidance in the table below to help the taxpayer complete the form:

	Section	Line Instruction
1.	A - Select One Box	<p>1. Box 1 is checked when the taxpayer is not a business owner and has not applied for an EIN. The taxpayer is receiving notices for an unknown business in their name with an assigned EIN.</p> <p>Note: If Box 1 is checked, the taxpayer should provide the 9-digit EIN being reported and complete Sections C, D, and F.</p> <p>2. Box 2 is checked when the taxpayer suspects the business entity, estate, trust, or exempt organization listed in Section B is a victim of identity theft.</p> <p>Note: If Box 2 is checked, the taxpayer should complete Sections B, C, D, E, and F.</p>

2.	B - My Business Information	<p>1. Legal name of entity: Provide the legal name of the business entity, estate, trust, or exempt organization.</p> <p>2. Approx. date entity established: Provide month/day/year, month/year, or year of establishment.</p> <p>3. EIN: Employer Identification Number</p> <p>4a-4d. Current business address: Provide the current address of the business including city, state and zip code.</p> <p>5. Tax forms affected: List the tax form(s) affected by identity theft (i.e., Form 1120, Form 940, Form 1041, Form 990).</p> <p>6. Tax year(s)/quarter(s) affected: List any year or quarter affected by identity theft (i.e., 2021, 202106).</p> <p>7. Previous names this entity was known by (if applicable): Provide any other names this entity was known by.</p> <p>8. Check only ONE of the following boxes:</p> <ul style="list-style-type: none"> • This EIN is currently Active (in business) • This EIN is currently Not Active - if operation ceased, provide the tax year/quarter of the final return filed in the space provided. <p>9. Check the box if the business was not required to file a tax return for the year/quarter they are reporting identity theft.</p>
----	-----------------------------	---

3.	Section C – Information of Individual Submitting This Form	<p>1. What is your position with the business entity/exempt organization shown below: Provide your position with the business entity (i.e., officer, director, sole member, executor, trustee, etc). The individual submitting the form must have the legal authority to act for the entity and to receive return information per IRC 6103.</p> <p>Note: If the taxpayer selected Box 1 in Section A, they should choose, 'Not applicable, I checked box 1 in Section A.'</p> <p>2. Your name: The name of the individual completing this form.</p> <p>3. Your Taxpayer Identification Number: Provide the 9-digit SSN or ITIN of the individual completing this form.</p> <p>4. Your mailing address: Provide the address of the individual completing this form, if different from Section A, Lines 4a-4d.</p> <p>5. Your Telephone number: Provide the phone number (including area code) of the individual completing the form. Indicate if the phone number is a home, work, or cell phone by checking the appropriate box.</p> <p>6. Best time(s) to call you: Indicate the best time for IRS to call, if necessary, and include time zone.</p>
4.	Section D - Reason for Filing this Form (Required)	Provide a detailed explanation of the identity theft incident, including relevant dates. The explanation does not need to be lengthy, but it should include all pertinent information as to why the taxpayer believes identity theft has occurred. If needed, attach additional information and/or pages to the form.

5.	Section E – Supporting Documentation	<p>1. If known, provide any information you have regarding the person(s) misusing your EIN or your name (i.e., provide the alleged perpetrator's name or address, or copy of a police report). Attach an additional sheet if necessary.</p> <p>2. Supporting Documents: Submit the completed form and a legible photocopy of the document(s) selected below to verify your identity. Check the box next to the documents being submitted. The documentation required is dependent upon the type of entity:</p> <ul style="list-style-type: none"> • Sole Proprietor (Two documents are required): Provide one document from box 'a' (passport, driver's license, or other valid U.S. Federal or State government issued identification with your signature and one document from box 'b' (copy of a utility bill, invoice, mortgage/rent receipt or other documentation to support business operation). <p>Note: Remind the caller not to submit photocopies of federally issued identification where prohibited by 18 U.S.C. 701 (i.e., official badges designating federal employment).</p> <ul style="list-style-type: none"> • Corporation, Partnership, Limited Liability Company, Exempt Organization, Estate or Trust: Provide one or more of the documents listed in this section (Articles of Incorporation, Articles of Organization, Trust or Estate document, or a statement signed by an officer or director (not the same person in Section C) on corporate letterhead stationery stating that the person in Section C has authority to legally bind the corporation).
----	--------------------------------------	---

6.	Section F - Signature	The form is signed and dated by the individual completing this form in Section C.
----	-----------------------	---

Note: Remind the caller that failure to provide required documentation with a signed Form 14039-B may delay processing.

- (3) If the taxpayer is submitting the Form 14039-B in response to a notice or letter received from the IRS, advise the taxpayer to send the completed Form 14039-B and any required documentation with a copy of the notice or letter to the address provided in that notice or letter.

Note: If the taxpayer is responding to a notice or letter from the IRS and it provides a fax number, advise the taxpayer to send the completed Form 14039-B and any required documentation with a copy of the notice or letter to the fax number shown on the notice or letter.

- (4) If the taxpayer did NOT receive a notice or letter from the IRS, advise the taxpayer to submit the form per the instructions on the Form 14039-B.

25.23.11.6.6
(10-01-2023)
BMF Identity Theft Referrals - AM BMF Identity Theft Teams Only

- (1) All the required research must be completed prior to referring the case to another function. This is to ensure that confirmed ID theft cases and cases with the high probability of ID theft can be placed in the correct inventory as quickly as possible.
- (2) Due to the potential complexity of a BMF ID theft, it may be necessary to refer the case to another function for either resolution or assistance. All functions have established BMF ID theft Liaisons to assist in the working of ID theft cases. To find a list of the functional liaisons, see the *BMF ID Theft Liaisons* located on the BMF ID Theft Website.
- (3) If working a paper case and the entire case is being referred to another function:
 - a. **DO NOT** close the control until the case has been accepted by the receiving function. This is to prevent the case from slipping through the cracks when moving the case from one function to another. Once the referral is accepted by the receiving function and all account actions are completed close the control.
- (4) All referrals will move from one functional liaison to another functional liaison. See IRM 25.23.9.3, BMF Identity Theft Liaisons, for additional information.
- (5) If the contact is received by phone, all of the required research is completed and the case is being referred, annotate the Form 14566 with "phone contact" so the liaison will be aware that no control will be open.
- (6) When assistance is needed from another function the control will remain open until the response is received. The receiving function must respond to the request within 30 days of receipt. See IRM 25.23.9.8, BMF ID Theft Referrals,

for additional information. If no response is received within 30 days of receipt by receiving function, follow-up should be elevated to the *BMF ID Theft Liaison*.

25.23.11.6.6.1

(10-01-2024)

Fabricated EINs

- (1) A fabricated EIN is an EIN established for a business that does not exist. The sole purpose of the fabricated EIN is to defraud the government through the filing of fraudulent BMF or IMF returns or income documents.
- (2) AM BMF IDT may lock an EIN suspected of being fabricated, often because of taxpayer contact (i.e., phone call stating they did not request the EIN or submitting Form 14039-B). There will be a posted TC 971 AC 524 on CC ENMOD containing BMF IP EINFAB in the MISC field. The taxpayer's entity will also be updated to include 'Identity Theft' in the sort name line.

Note: AM BMF Identity Theft always includes 'Identity Theft' in the sort name line when deeming an account fabricated.

- (3) RICS may lock an EIN suspected of being fabricated and issue Letter 5263C, Entity Fabrication, requesting additional information to verify the entity. There will be an open control assigned on CC ENMOD to 1481400000 with a category code of TPPI and activity code showing potential entity fabrication (POTENTEF). There will also be a posted TC 971 AC 524 on CC ENMOD containing EINFAB2 in the MISC field.

Note: TC 971 AC 524 containing BMF RICS EINFAB in the MISC field deemed fabricated by RICS will include 'POTENTIAL FAB EIN' in the sort name line. TC 971 AC 524 containing BMF RICS EINFAB2 deemed fabricated by RICS may or may not include 'POTENTIAL FAB EIN' in the sort name line.

- (4) If the taxpayer submits a paper inquiry or a phone call is received, and the account contains the indicators listed above, non-specialized IDT teams follow the If/Then chart below:

	If	Then
1.	An inquiry is received via paper or phone and a Fabricated EIN determination has been made	Prepare Form 14566, BMF Identity Theft Referral, and send by secure email to the AM BMF IDT liaison at <i>*TS AM BMF IDT</i> . In the subject line of the secure email, include the tax year of the case that is being referred.
2.	An inquiry is received via paper or phone and a Fabricated EIN determination has been made and the account includes CI involvement (-Z freeze, etc.)	Prepare Form 14566, BMF Identity Theft Referral, and send by secure email to the AM BMF IDT liaison at <i>*TS AM BMF IDT</i> . Note: The referral must include the account has CI involvement.

#

- (6) If the taxpayer calls about their EIN where a letter 5263C was issued and account contains the indicators listed above, all AM BMF CSRs should follow the If/Then chart below.

	If	Then
1.	Taxpayer claims they have no knowledge of the business referenced on the letter, questions the letter, or is asking for assistance related to the letter	Advise the TP they must reply to the 5263C letter and provide the requested information via FAX or to the address provided on the letter.
2.	Taxpayer states they did not receive the 5263C letter	<p>2. Explain to the TP they must respond to the letter providing the requested information.</p> <p>3. Advise the TP they should receive the re-issued letter within 30 days</p>

#

#

Note: The remainder of the procedures below are only for AM BMF CSRs trained in BMF Identity Theft.

- (7) If a referral is needed to lock an account due to a fabricated EIN, only one referral is required.
- (8) If a fabricated EIN is a sole proprietorship, remove the sole proprietor link to the cross-reference SSN.
- (9) Refer to IRM 25.23.9.8.1, Fabricated or Inactive Employer Identification Number (EIN) Procedures, for the required account actions needed prior to requesting the account be locked.

Step	Action
1	Document all of your findings on the Form 14566, BMF Identity Theft Referral.
2	Be certain to include all appropriate research completed on the referral form and explain any IMF implications if applicable.
3	On the subject line of the referral enter: TC 971 AC 524 and CII Case ID if available.
4	Send the completed referral to your AM BMF Identity Theft liaison by secure e-mail using the <i>*TS AM BMF IDT</i> mailbox, for referral to IP, the Entity Fabrication (EF) Team in RICS, and CI. The email must also contain a PDF print of the original entity (CC ENMOD), including filing requirements, when submitting the referral to the AM BMF Identity Theft liaison. Reminder for EO employees working IDT: If an EO account is being locked, the EO subsection must be removed from the entity prior to the account being locked. The referral would first be sent to your liaison per the <i>BMF ID Theft Liaisons</i> located on the BMF ID Theft Website on SERP.
5	Document the sending of the referral on AMS along with the details of the request. If working a CII case, attach the referral and the PDF print of the original entity (CC ENMOD) to the case.

- (10) If an account previously deemed fabricated by AM has been locked in error, or an inactive account needs to be unlocked, send a referral to the AM BMF ID Theft liaison by secure e-mail using the **TS AM BMF IDT* mailbox to have the TC 971 AC 524 reversed.

Step	Action
1	Document your findings on the Form 14566, BMF Identity Theft Referral.
2	Include all appropriate research completed on the referral and explain why the account needs to be unlocked.
3	On the subject line of the referral, enter: TC 972 AC 524 and CII Case ID if applicable.
4	Research CII for the original case and, if available, attach the PDF print of the original entity (CC ENMOD) to the secure e-mail. If the original case does not have a PDF print of the original entity attached, notate in the referral that the information was not available.

5	Send the completed referral to your AM BMF Identity Theft liaison by secure e-mail using the <i>*TS AM BMF IDT</i> mailbox, for referral to IP, Entity Fabrication (EF) Team in RICS, and CI.
6	Document the sending of the referral on AMS along with the details of the request. If working a CII case, attach the referral to the case.
7	Once IP confirms the account has been unlocked, monitor the case until the TC 012, TC 971 AC 524, and the corrected sort name line are posted.

- (11) There will be times when the fraudulent Forms W-2 have been filed under a valid business's EIN. An additional referral may be needed to the Combined Annual Wage Reporting (CAWR) group. See the following IRM for these procedures:

- IRM 25.23.9.8.5, Referrals to Combined Annual Wage Reporting (CAWR)

- (12) RICS may make a determination that the EIN is fabricated and send a Form 14566 to clean up the account.

- RICS inputs 'Potential FAB EIN' on the sort name line when they make the determination and then locks the EIN with a TC 971 AC 524.
- RICS will complete a separate Form 14566 for each EIN with the request to back out the account.
- BMF IDT SME's will follow the guidance on the Form 14566 and back out account, resolving any balance dues, credit or payments on the account.

Note: No other actions are required unless specifically stated on the Form 14566 (for example, input of TC 971 AC 504 on the XREF SSN or removal of the sole proprietor link to the XREF SSN).

- If Z freeze is present, input all adjustments as requested.
- After the adjustments have been input, if there is a Z freeze present, respond to the e-mail and include the IDT liaisons for BMF Refund Crimes and RICS in the response (*BMF IDT Liaison*). Include in the body of the e-mail for CI to force post the adjustment. Monitoring for the posting is not required.

Note: If CI doesn't force post, and the unpostable is deleted then they will send an e-mail to re-input the adjustments. Follow same procedures above.

25.23.11.6.6.2
(05-04-2022)

**Collection Activity -
Form 13794 Additional
Actions Required - Lien
-AM BMF Identity Theft
Teams only**

- (1) If there is a TC 582 (Lien Indicator) or TC 360 (Lien Fee Assessment) posted and a full abatement will reverse the tax liability to zero, prepare Form 13794, Request for Release or Partial Release of Notice of Federal Tax Lien. Form 13794 should be completed and forwarded to the Collection Advisory.

Note: Only Collection Advisory has the authority to reverse lien fees (TC 360) on accounts impacted by IDT.

(2) Take the following actions when completing the Form 13794:

- a. Input as much information as possible regarding the abatement

Note: Include specific instruction for the lien and/or lien fee reversal on the Form 13794 in section "Date lien satisfied or resolved (e.g., payment date, adjustment posting date, discharge date)". For example, *Request IDRS input TC 583 & TC 361 \$X.XX for MFT/Tax period.*

- b. Include the Serial Lien Identification (SLID) Number from the Notice of Federal Tax Lien, if available
- c. Check box 9 indicating "Erroneous Lien"
- d. Include "ID Theft" in the "Reason" box
- e. Fax/EE-Fax or e-mail Form 13794 to the Collection Advisory Unit for the state where the taxpayer currently resides. Include the specifics of your request as mentioned above also in the body of the Fax/EE-Fax, so it appears on the cover sheet.

Note: If you do not have access to the Automated Lien System (ALS), include a note asking Advisory to complete the SLID and TSIGN.

- f. Attach completed Form 13794 to the CII case and leave a case note with the date the form was faxed and to which Advisory.

(3) Collection Advisory contacts can be found under the Who/Where tab on the SERP Home Page on the *Advisory Units Contact List*.

Reminder: When adjusting an IDT account where a NFTL was filed on the account (TC 582 posted) and a tax liability remains after the account has been adjusted the NFTL will remain in place. The NFTL will be systemically released when the account balance is satisfied (zero).

(4) The Advisory Unit will review the Notices of Federal Tax Lien (NFTL) filed against the taxpayer using the Automated Lien System (ALS). If all modules on the NFTL are satisfied, Advisory will request the release of the NFTL as an erroneously filed NFTL per IRC 6326(b). The release of the NFTL will reverse the TC 582. Advisory will abate the TC 360 associated with the NFTL filing and issue Letter 544, Letter of Apology - Erroneous Filing of Federal Tax Lien, to the taxpayer.

Note: Routing of the Form 13794 is required to be documented in a CII or AMS case note.

(5) If it has been more than 30 days since the lien release posted and the taxpayer has any issue with requests for the Notice of Federal Tax Lien (NFTL) to be released, refer the taxpayer to Publication 1450, Instructions for Requesting a Certificate of Release of Federal Tax Lien, to submit a written request for Certificate of release of erroneously filed Notice of Federal Tax Lien. The release date can be calculated based on the posting of the reversal of the TC 582 and TC 360.

25.23.11.6.7
(10-01-2023)

**Account Actions - AM
BMF Identity Theft
Teams Only**

- (1) Once ID theft has been established and the case reviewed by the manager or lead, it will be necessary to correct the account.
- (2) **If the invalid return has posted first and valid return posted as a “DUPF”:**
 1. Determine if ASED needs to be added prior to inputting any adjustment. On duplicate returns it may be necessary to update the ASED to reflect the correct received date of the valid return. The ASED will need to be updated if it is different from the date posted on the original return on the module. The ASED will need to be updated to the received date plus 3 years. Input the ASED with a TC 560 using CC REQ77 as appropriate. See IRM 25.6.1.6.14, Criteria for Establishing a Statute of Limitations Period, for additional information.

Example: The return due date is 04-15-2020 and the ID Theft original return posted 04-14-2020. The ASED for this return would be 04-15-2023. The true taxpayer had filed an extension on 04-10-2020. The valid return was received on 08-14-2020, the ASED for the valid return would be updated to 08-14-2023.
 2. Completely back out (nullify) the invalid return first. This is to have the adjustment notice reflect the adjustment to the taxpayer's figures. **Do not** net the returns. Input the adjustment with a HC 4 to hold the notice and any credit that may be on the module.
 3. Reverse any offsets in or out of the module if appropriate. Always input a secondary TC 570 on any credit transfers being moved into the ID theft module. This will hold the credit if necessary.
 4. If any refund was lost as a result of the filing of the ID theft return additional procedures will need to be completed in order to balance the valid taxpayer's account. If the refund has already been released to the invalid TP the backing out of the return will create a debit on the module. To balance the account, credit from the 1545 account will need to be moved into the account once the invalid return is backed out. Input command code IDT48 (to reverse a fraudulent refund to the taxpayer affected by IDT) or IDT58 (to reverse a partial refund to the taxpayer affected by IDT) and suspend the case until the TC 841 posts back to the account. See IRM 25.23.9.9.6, Lost Refund, for input procedures. The credit will be returned to the module as a TC 841- entire refund lost, TC 700 partial refund lost. Monitor the case until the TC 841/700 posts back to the account.
 5. If the refund was lost, input a TC 470 with a post delay of 1 cycle. This will prevent the issuance of any collection notices until the credit is moved in from the 1545 account.
 6. Math verify the valid return to ensure there are no errors. If there is a math error, follow normal adjustment math error procedures.
 7. Once the TC 841/700 posts back to the account, adjust the account to reflect the valid taxpayer's return. If the return is a refund or isn't going to result in a balance due, use HC 0 to allow the adjustment notice to generate to the taxpayer. If the valid taxpayer's return is going to result in a balance due:
 1. Determine if the return was timely filed. If the return was late you will need to manually calculate and assess any applicable failure to file (FTF) penalty. See IRM 20.1.2.2.1, When Timely mailing Equals Timely Filing or Paying (Received Date vs. Filing /Payment Date).

2. Input adjustment using PC 2. This allows the computer to recognize the need to compute the FTP back to the return due date.
3. Input the adjustment with the appropriate IRN 871 amount. The amount listed for the IRN 871 is the tax shown on the taxpayer's valid return.
4. For more details on the procedures, see IRM 25.23.11.6.8, Invalid Return Posted First and the Valid Return is a Balance Due.
8. Determine if the address is correct. If address was changed as a result of the ID theft return, correct it back to the taxpayer's correct address.
9. Once the TC 841/700 posts, review the account to ensure all account issues have been corrected or addressed with the taxpayer.
10. Input TC 971 AC 522 CLSIDT.
11. Send Letter 5317C to explain to the taxpayer all actions taken.

(3) Only the invalid return is posted:

1. Back out the invalid return. Use HC 4 to hold the notice.
2. Reverse any offsets in or out of the module if appropriate. Always input a secondary TC 570 on any credit transfers to hold any credits being moved into the ID theft module.
3. If the refund was lost, Input a TC 470 with a post delay of 1 cycle. This will prevent the issuance of any collection notices until the credit is moved in from the 1545 account.
4. If any refund was lost as a result of the filing of the ID theft return additional procedures will need to be completed in order to balance the valid taxpayer's account. Input command code IDT48 (to reverse a fraudulent refund to the taxpayer affected by IDT) or IDT58 (to reverse a partial refund to the taxpayer affected by IDT) and suspend the case until the TC 841/700 posts back to the account. See IRM 25.23.9.9.6, Lost Refund, for procedures. Monitor the case until the TC 841/700 posts back to the account.
5. If there are payments on the account, research the payments to ensure they are not misapplied. If they are, move them to the correct account. If you are unable to determine where a payment should be applied, move the payments to the Unidentified Remittance File or Excess Collection File per IRM 21.5.7.3.5, Researching Unidentified Remittances and Excess Collection File.
6. Determine if the address is correct. If address was changed as a result of the ID theft return, correct it back to the taxpayer's correct address.
7. Review the account to ensure all account issues have been corrected or addressed with the taxpayer.
8. Input TC 971 AC 522 CLSIDT.
9. If EIN is active but there are no filing requirements or the taxpayer has no filing requirements for that specific form, close the appropriate filing requirements.
10. Send Letter 5317C to explain to the taxpayer all actions taken.

(4) ID theft return is an amended return:

1. Reverse the adjustment input for the amended return. Use a HC 3 to hold the notice.
2. Reverse any offsets in or out of the module if appropriate. Always input a secondary TC 570 on any credit transfers to hold any credits being moved into the ID theft module.

3. If the refund was lost, input a TC 470 with a post delay of 1 cycle. This will prevent the issuance of any collection notices until the credit is moved in from the 1545 account.
 4. If any refund was lost as a result of the filing of the ID theft return additional procedures will need to be completed in order to balance the valid taxpayer's account. Input command code IDT48 (to reverse a fraudulent refund to the taxpayer affected by IDT) or IDT58 (to reverse a partial refund to the taxpayer affected by IDT) and suspend the case until the TC 841 posts back to the account. See IRM 25.23.9.9.6, Lost Refund, for procedures. Monitor the case until the TC 841 posts back to the account.
 5. Determine if the address is correct. If address was changed as a result of the ID theft return, correct it back to the taxpayer's correct address.
 6. Review the account to ensure all account issues have been corrected or addressed with the taxpayer.
 7. Input TC 971 AC 522 CLSIDT.
 8. Send Letter 5317C to explain to the taxpayer all actions taken.
- (5) In all cases where it has been determined the EIN is fabricated and the account needs to be locked, see IRM 25.23.11.6.6.1, Fabricated EIN Referrals, for procedures. Using CC ENREQ, input "Identity theft" on the second name line (sort name) to identify this account as fabricated.

25.23.11.6.8
(10-01-2023)

**Invalid Return Posted
First and the Valid
Return is a Balance Due**

- (1) There will be situations where an ID theft return posted first and the valid taxpayer's return is a balance due and the tax was paid late or still unpaid. In these situations, failure to pay (FTP) penalties must be charged.

#

- (3) If the valid taxpayer's return was filed late, it will still be necessary to manually compute the FTF penalty.
- (4) Math verify the return.
- (5) It is important the correct information is entered on the adjustment to ensure the correct charging of the FTP penalty.

Step	Action
1	Back out the invalid return. DO NOT net the returns. Back out any associated penalties with the exception of bad check penalty (TC 280) or the FTP penalty charged on the TC 150. The FTP will automatically recompute once the back out adjustment posts. Exception: Netting can be done if the ASER is imminent.
2	Follow procedures in IRM 25.23.11.6.7 (2), Account Actions - AM BMF Identity Theft Teams Only, for all other needed account actions. The only difference in working the balance due returns where FTP penalty needs to be assessed is on the REQ54 input for the valid return. The new aspects of the adjustments are: 1. The use of priority code (PC 2) on the adjustment- PC 2 advises the computer that the FTP needs to be computed back to the RDD. 2. The IRN 871- The amount of the IRN 871 represents the "tax shown" on the valid return minus refundable credits. The IRN 871 amount tells the computer to compute the FTP based on the lesser of the IRN 871 amount (what the taxpayer expected to owe) or the tax assessed (290 amount) on the return from the due date of the return. In the computation of FTP penalty, the computer will recognize FTD and ES payments and refund reversals (TC 841/700) and calculate the FTP penalty appropriately.
3	Use HC 0 to allow the adjustment notice to generate.
4	If multiple account actions are being taken, post delay the adjustment for 1 cycle to allow all actions to post prior to the adjustment.

Example: Invalid return posted first. The taxpayer's valid return shows a balance owed of \$1,000. However, after the valid return was math verified the true balance owed is \$1,500. The adjustment would be a TC 290 for \$1,500 using the IRN 871 for \$1,000 (tax shown on the valid return) and PC 2. The computer will determine the lesser of the tax assessed (\$1,500) and the "tax shown" (\$1,000). The computer will compute the FTP on the IRN 871 amount of \$1,000 back to the return due date. Since the taxpayer was not aware of the additional \$500 owed the taxpayer has the 21 days from the 23C date to pay before FTP is assessed.

Example: The taxpayer made ES payments totaling \$5,000. The invalid return posts claiming a \$4,000 refund. With the ES payments made, a refund is issued for \$9,000 to the identity thief. After the return is backed out and the \$9,000 is credited from the 1545 account, there will be a \$5,000 credit on the module. There is \$7,000 "tax shown" on the valid return with no refundable credits. Since there is no math error on the return the IRN 871 will be \$7,000 also. The adjustment will be a TC 290 \$7,000

with, IRN 871 \$7,000 with PC 2 HC 0. The computer will recognize the \$5,000 in ES payments and charge FTP on \$2,000 from the RDD to the date the account is paid in full.

- (6) For additional information, see IRM 25.23.9.9.4, Invalid Return Posted First and the Valid Return is a Balance Due.

25.23.11.6.9
(10-01-2020)
Lost Refund

- (1) If an ID theft return (original or amended) has been processed and as a result a refund was issued to the Identity thief, credit back the ID theft refund amount into the taxpayer's account in order to balance the account. This is done by moving credit from the ID theft 1545 account.
- (2) Prior to moving the credit into the account, reverse all available offsets that occurred.
- (3) To move the credit from the 1545 account, input command code IDT48 (to reverse a fraudulent refund to the taxpayer affected by IDT) or IDT58 (to reverse a partial refund to the taxpayer affected by IDT) as applicable.
- (4) If part of the refund was offset and the credit is being returned to the module, only the portion of the refund that is unrecoverable will be moved from the 1545 account.
- (5) To input the reversal using command codes IDT48 or IDT58:
 - See IRM 2.4.61-1, IDT48, RPM48 or CSO48 Input Format
 - See IRM 2.4.61-2, IDT58, RPM58, CSO58 Input Format
- (6) Suspend case and monitor for the posting of the TC 841/700. This is usually 2-4 weeks.
- (7) The preparation and posting of the TC 841 should be completed prior to backing out the return if possible.

25.23.11.6.10
(10-01-2018)
Reversing TC 130

- (1) Only those trained in working ID Theft cases can reverse a TC 130 and will follow guidance below.
- (2) If identity theft is confirmed, thoroughly research all related accounts for legitimate outstanding balances prior to reversing any TC 130 on the account. Ensure there are no balances on the IMF, BMF or NMF account. See IRM 25.23.11.4.1, Accounts Containing TC 130 for research steps.
- (3) Prior to inputting the TC 131, forward case to manager or lead for approval.
- (4) The manager or lead will review the case information and determine if the reversal is appropriate. The manager or lead will leave a CII message on the case with the facts that back up the decision to allow or disallow the reversal of the TC 130.
- (5) If no liabilities remain on IDRS or NMF, input the TC 131 to ENMOD using CC REQ77.

25.23.11.6.11
(10-01-2019)

**Reversing BMF Identity
Theft Indicators**

- (1) If a BMF identity theft (IDT) indicator (TC 971 AC 522) was erroneously entered on an account, subsequent research determines no ID theft has occurred or the taxpayer doesn't respond to the request for additional information, reverse the ID theft indicator. Reverse using a TC 972 AC 522. Use the appropriate MISC code to reflect the reason for the reversal.
 - NOIDT- After researching the account it is determine no ID theft exists. Document on AMS/CII why ID Theft is not indicated
 - NORPLY- Taxpayer does not respond to the request for additional information
 - IRSERR- Indicator input incorrectly
 - FALSE- It is determined the taxpayer is falsely claiming ID theft
 - OTHER- Any reason not listed above. Document AMS/CII with reason for reversal
- (2) For additional information see exhibit in IRM 25.23.9-5, Reversing BMF Identity Theft Indicators-TC 972 AC 522.

Business Master File (BMF) Identity Theft Procedures for Accounts Management 25.23.11

page 65

Exhibit 25.23.11-1 (10-01-2023)

Accounts Management Form 14566 Instructions

The table below will assist the Accounts Management Customer Service Representative with initiating the Form 14566, BMF Identity Theft Referral. The Accounts Management *BMF IDT Liaison* will review the form, complete the remaining fields, and forward to the appropriate functional BMF IDT Liaison.

Form 14566 Field Name	Field Data
Liaison Name	Enter the name of the liaison where the referral is being sent
Liaison Function	Select function where referral is being sent from the drop down menu options.
Business Information	Include Business EIN, Name and Address.
Claimant Information	Include Claimant SSN, Name/Title, Address and Phone number.
Account Information	Include CII number (when applicable), MFT and Tax period/s.
Actions Requested	Check all actions being requested. Note: There are only 2 actions listed under “IMF Actions”. All other actions are BMF.
Explanation for ID Theft Determination (Required Field)	It is very important to provide a detailed explanation to the receiving function of what was found that this case was determined as IDT and what specific actions you are requesting. Attach documents that prove your determination when available, and if Form 14039 or Form 14039-B is present, attach the form to the secure e-mail. Note: It is helpful to also indicate whether the <i>IAT BITR Tool</i> was used to make the IDT determination.
Employee Name and Function	Full name of person submitting the Form 14566 and the function they belong to.
Telephone Number	Phone number of initiator in case contact needs to be made.
Date	Date the Form 14566 is prepared and/or sent.

