



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

25.23.9

AUGUST 25, 2025

EFFECTIVE DATE

(10-01-2025)

PURPOSE

- (1) This transmits revised IRM 25.23.9, Identity Protection and Victims Assistance, BMF Identity Theft Processing.

MATERIAL CHANGES

- (1) IRM 25.23.9.1.4 - Added new subsection for Program Controls. Remaining subsections renumbered.
- (2) IRM 25.23.9.2 - Changed the note in paragraph one from a high probability of ID theft to a possibility of ID theft.
- (3) IRM 25.23.9.3 - Updated an old link to the BMF IDT Liaison Contacts with new link. Added a new link for the new Who/Where Liaison Contacts page. IPU 24U1037 issued 10-11-2024.
- (4) IRM 25.23.9.4.1 - Added a note regarding the definition of a TC 971 AC 123 and what actions should be taken. Also, updated RICS category code from TPPI to BIDT.
- (5) IRM 25.23.9.5.1 - Changed paragraph 6 to include all ID theft inquiries made by the taxpayer need an acknowledgement letter sent.
- (6) IRM 25.23.9.6 - Updated the criteria for when to input a TC 971/522 in paragraph 1. Updated the IDTCLM definition in the chart.
- (7) IRM 25.23.9.6 - Added Action Code 524 with Tax Administration Code ENTLOK and definition to the chart. IPU 25U0052 issued 01-14-2025.
- (8) IRM 25.23.9.6.1 - Removed a sentence in paragraph 1 regarding tax implications and ID theft.
- (9) IRM 25.23.9.7 - The table was changed from a high probability of ID Theft to a possibility of ID Theft.
- (10) IRM 25.23.9.8.1 - Added more information to the inactive accounts portion in paragraph 5.
- (11) IRM 25.23.9.8.4 - Added that a TC 971 AC 504 SPCL2 needs to be input on the SSN of the cross reference for the EIN to the list in paragraph 4.
- (12) IRM 25.23.9.8.4 - Input an exception stating a TC 020 will not post when a TC 971 AC 524 with miscellaneous code ENTLOK is used. IPU 25U0052 issued 01-14-2025.
- (13) IRM 25.23.9.9 - Updated old link to the BMF IDT Liaison Contacts with the new link to the new SERP page. IPU 24U1037 issued 10-11-2024 IRM.
- (14) IRM 25.23.9.9 - _ Added a link to the SERP page for Collection Advisory Contact List.
- (15) IRM 25.23.9.10.3 - Added new subsection regarding BMF TDS transcripts when identity theft indicators are present. IPU 25U0052 issued 01-14-2025.
- (16) Exhibit 25.23.9-1 - Added new TC 971 AC 524 code ENTLOK and definition to chart. IPU 25U0052 issued 01-14-2025.

- (17) Various editorial changes have been made throughout the IRM. Reviewed and updated grammar, web addresses, organizational terms and titles, and IRM references where applicable. IPU 24U1037 issued 10-11-2024 IRM 25.23.9.

EFFECT ON OTHER DOCUMENTS

IRM 25.23.9, BMF Identity Theft Processing, effective as 10-1-2024 is superseded. The following IRM procedural Updates (IPU), 24U1037 issued on 10-11-2024, and 25U0052 issued on 1-14-2025 have been incorporated into this IRM.

AUDIENCE

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

Lucinda Comegys
Director, Accounts Management
Taxpayer Services Division

25.23.9

Business Master File (BMF) Identity Theft Processing

Table of Contents

25.23.9.1 Program Scope and Objectives

25.23.9.1.1 Background

25.23.9.1.2 Authority

25.23.9.1.3 Roles and Responsibilities

25.23.9.1.4 Program Control

25.23.9.1.5 Terms and Acronyms

25.23.9.1.6 Related Resources

25.23.9.2 Business Master File (BMF) Identity Theft - Overview

25.23.9.2.1 Non-Tax related Identity Theft

25.23.9.3 Business Master File (BMF) Identity Theft Liaisons

25.23.9.4 Business Master File (BMF) Identity Theft Research (Inquiry received via paper or phones)

25.23.9.4.1 BMF Returns Selected for Return Integrity and Compliance Services (RICS) Review

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

25.23.9.5 Identity Theft Case Building- Business Master File (BMF)

25.23.9.5.1 Controlling Business Master File (BMF) Identity Theft Cases

25.23.9.5.2 Tracking Business Master File (BMF) Tax-Related Identity Theft Inventory

25.23.9.6 Business Master File (BMF) Identity Theft Tracking Indicators

25.23.9.6.1 Allegation or Suspicion of Business Master File (BMF) Identity Theft Transaction Code (TC) 971
Action Code (AC) 522 IDTCLM

25.23.9.6.2 Taxpayer Supporting Documentation - Transaction Code (TC) 971 Action Code (AC) 522
IDTDOC

25.23.9.6.3 Closing Business Master File (BMF) Identity Theft Issues- Transaction Code (TC) 971 Action
Code (AC) 522 CLSIDT

25.23.9.6.4 Locking Accounts- Transaction Code (TC) 971 Action Code (AC) 524

25.23.9.6.5 Reversing Business Master File (BMF) Identity Theft Indicators

25.23.9.6.6 Reversing Business Master File (BMF) Identity Theft Indicators - Transaction Code (TC) 972
Action Code (AC) 522 NORPLY

25.23.9.6.7 Reversing Business Master File (BMF) Identity Theft Indicators - Transaction Code (TC) 972
Action Code (AC) 522 NOIDT

25.23.9.7 Form 14039-B, Business Identity Theft Affidavit

25.23.9.7.1 Complete and Legible Documents

25.23.9.8 Business Master File (BMF) Identity Theft Referrals

25.23.9.8.1 Fabricated or Inactive Employer Identification Number (EIN) Procedures

25.23.9.8.2 Referrals to Return Integrity and Compliance Services (RICS)

-
- 25.23.9.8.3 Referrals to Criminal Investigation (CI)
 - 25.23.9.8.4 Referrals to Lock the Account
 - 25.23.9.8.5 Referrals to Combined Annual Wage Reporting (CAWR)
 - 25.23.9.9 Account Actions
 - 25.23.9.9.1 Duplicate /Amended Return Research
 - 25.23.9.9.2 Invalid Return Posted First and Valid Return (Refund or Zero Balance)
 - 25.23.9.9.3 Posted Return on Either a Fabricated Employer Identification Number (EIN) or Inactive Account
 - 25.23.9.9.4 Invalid Return Posted First and the Valid Return is a Balance Due
 - 25.23.9.9.5 Statute Implications
 - 25.23.9.9.6 Lost Refund
 - 25.23.9.9.7 Request for a New Employer Identification Number (EIN) by a Taxpayer Who Is a Victim of Identity Theft
 - 25.23.9.10 Providing Copies of Tax Returns or Income Documents Where ID Theft is Suspected or Proven
 - 25.23.9.10.1 Sending Redacted Information
 - 25.23.9.10.2 Redacting Information
 - 25.23.9.10.3 BMF Transcripts and Identity Theft

Exhibits

- 25.23.9-1 Transaction Code (TC) 971 Action Code (AC) 5XX- MISC Codes
- 25.23.9-2 Business Master File (BMF) Identity (ID) Theft Indicators - Transaction Code (TC) 971 Action Code (AC) 522 IDTCLM - Initial Allegation or Suspicion of Business Master File (BMF) Identity (ID) Theft
- 25.23.9-3 Business Master File (BMF) Identity (ID) Theft Indicators - TC 971 AC 522 IDTDOC - BMF ID Theft Documents Accepted
- 25.23.9-4 Business Master File (BMF) Identity (ID) Theft Indicators - TC 971 AC 522 CLSIDT - Closed and Confirmed as BMF ID Theft
- 25.23.9-5 Reversing Business Master File (BMF) Identity (ID) Theft Indicators - Transaction Code (TC) 972 Action Code (AC) 522
- 25.23.9-6 Business Master File (BMF) Identity Theft Referral Form
- 25.23.9-7 Business Master File (BMF) Identity Theft Research Requirement

25.23.9.1
(09-15-2020)
Program Scope and Objectives

- (1) **Purpose:** This manual provides procedures for Business Master File (BMF) identity (ID) theft inventory cases and assisting victims of identity theft through taxpayer written correspondence, phone or face to face contacts.
- (2) **Audience:** The primary users of this IRM are all IRS employees in business operating divisions (BODs) who interact with taxpayers who may experience business related Identity (ID) theft by telephone, correspondence, or in person. These employees are in Small Business/Self Employed (SB/SE), Taxpayer Services (TS), Large Business and International (LB&I), Tax Exempt and Government Entities (TE/GE) and Criminal Investigations (CI) in the following functions: Accounts Management (AM), Submission Processing (SP), Collection, Exam, and Taxpayer Assistance Center (TAC).
- (3) **Policy Owner:** Director, Customer Account Services.
- (4) **Program Owner:** Identity Protection Strategy & Oversight is the internal organization responsible for the administration, procedures and updates related to BMF identity theft.
- (5) **Primary Stakeholders:** Accounts Management (AM), Taxpayer Assistance Center (TAC), Collection, Exam, and Return Integrity and Compliance Services (RICS) employees.
- (6) **Program Goals:** To quickly and effectively resolve Business Master File (BMF) accounts where ID theft is claimed or identified.

25.23.9.1.1
(09-12-2017)
Background

- (1) Business Master File (BMF) Identity (ID) Theft can involve the use of business's information to file fraudulent returns to support Individual Master File (IMF) ID theft or to obtain refunds from BMF accounts. A person can use an individual's stolen personal information to obtain an Employer Identification Number (EIN) to file false BMF tax returns and income documents. BMF accounts include the following entity types: sole proprietorship, limited liability company (LLC), corporation, partnership, estate, trust, exempt organization, or government entity.

25.23.9.1.2
(10-01-2024)
Authority

- (1) Policy Statement 10-1 (formerly P-25-1), IRM 1.2.1.17.1, Assisting taxpayers who report they are victims of identity theft. The Internal Revenue Service shall take the necessary steps to provide help to victims of identity theft within the scope of their official duties. Where appropriate, the Internal Revenue Service shall encourage victims to report instances of identity theft to other Federal agencies. The Internal Revenue Service recognizes the need for consistency across its functions to ensure the timely resolution of taxpayer account issues stemming from identity theft. In addition, identity theft victims shall be advised of the impact, if any, on their future filing requirements.
- (2) The *Taxpayer Advocate Service* 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.

25.23.9.1.3
(10-01-2021)

**Roles and
Responsibilities**

- (1) Any employee who handles cases where the taxpayer says they are a victim of BMF ID theft, or the employee identifies BMF ID theft is responsible for following the procedures set forth in this IRM.

25.23.9.1.4
(10-01-2025)

Program Control

- (1) Goals, measures and operating guidelines are provided in the yearly Program Letter. Quality data and guidelines for measurement is referenced in IRM 21.10.1, Embedded Quality (EQ) Program for Taxpayer Services, Campus compliance, Field Assistance, Tax Exempt/Government Entities, Return Integrity And Compliance Services (RICS) and Electronic Products and Services Support.

25.23.9.1.5
(10-01-2024)

Terms and Acronyms

(1) **Acronyms**

- AMS- Accounts Management Services
- BISTR- BMF Identity Theft Research
- BMF- Business Master File
- BOD- Business Operation Division
- CC- Command Code
- CCC- Computer Condition Code
- CI- Criminal Investigation
- CII- Correspondence Imaging Inventory
- EIN- Employer Identification Number
- IDT- Identity Theft
- IMF- Individual Master File
- IP - Identity Protection
- IPSO- Identity Protection Strategy and Oversight
- ITIN- Individual Taxpayer Identification Number
- LLC- Limited Liability Company
- OAR-Operations Assistance Request
- PII- Personally Identifiable Information
- RICS- Return Integrity and Compliance Services
- SFR- Substitute For Return
- SLA- Service Level Agreement
- SP- Submission Processing
- SSN- Social Security Number
- TAS- Taxpayer Advocate Service
- TBOR - Taxpayer Bill of Rights
- TS- Taxpayer Services

(2) **Definitions**

- Fabricated EIN- This is an EIN established for the sole purpose of defrauding the government by the filing of 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.
- Inactive EIN- An Inactive EIN belongs to a legitimate business whose business operations have ceased.
- 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.

- Fraud- Fraud is when a true owner of the EIN or authorized party tries to file false tax documents to receive a refund, reduce a tax liability, or receive other tax benefit to which they are not entitled.
- BMF Identity Theft- is defined by the filing of a Business Tax Return when someone creates, uses, or tries to use a business's or individual's identifying information without authority to obtain tax benefits.

25.23.9.1.6
(11-06-2020)
Related Resources

- (1) IRM 25.23.1.6, Data Breach Business Entities
- (2) Federal Trade Commission - <https://www.identitytheft.gov>
- (3) Social Security Administration - www.ssa.gov
- (4) *BMF Identity Theft Research (BITR)- BITR Tool*

25.23.9.2
(10-01-2025)
**Business Master File
(BMF) Identity Theft -
Overview**

- (1) Prior to validating BMF identity (ID) theft, extensive research **MUST** be performed to support the ID theft determination. BMF ID theft cases are extremely complex in nature and may require the research and analysis of both the business account and any individual accounts associated with the EIN. Cases may frequently involve multiple BOD/Functions as well. Refer to 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, for more information.

Note: The BMF ID theft tracking indicator, TC 971 AC 522, is input after thorough research shows there is a possibility of ID theft, , or the ID theft inquiry has been taken into a BMF ID theft treatment stream. The ID theft indicators will be input on the TXMOD for all accounts and MFTs where ID theft is suspected. The criteria for determining BMF ID Theft will be based on the guidance provided by each function's IRM. See IRM 25.23.9.6, Business Master File (BMF) Identity Theft Tracking Indicators .

- (2) BMF ID theft procedures must be followed when there is a tax related impact. Tax impact would include (this list is not all inclusive):
 - a. Fraudulent returns filed. This includes original or amended returns
 - b. Fraudulent income documents filed by an unauthorized party. This would include Forms W-2, Wage and Tax Statement, Form 1099 - MISC., Miscellaneous Income 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 IRM 25.23.9-7, Business Master File (BMF) Identity Theft Research Requirement.

- c. Fraudulent filing of Form 2848, Power of Attorney and Declaration of Representative and Form 8821, Tax Information Authorization.
- (3) For procedures for non-tax related ID theft see IRM 25.23.9.2.1, Non-Tax Related ID Theft.
- (4) IMF identity theft victims contact the IRS concerning their tax refunds. BMF taxpayers are often unaware their identities have been compromised until a notice or bill from the IRS is received. Taxpayers may contact the IRS when

they receive an unexpected notice about an inactive EIN or a levy notice relating to an EIN they never applied for or for a business they closed years ago.

- (5) 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 more information about the TBOR, see <https://www.irs.gov/taxpayer-bill-of-rights>.
- (6) On August 1, 2020, Form 14039-B, Business Identity Theft Affidavit, was published on IRS.gov for public access. Prior to this date, the form was sent to the taxpayer to obtain more information to validate their identity theft claim. Taxpayers may submit Form 14039-B, Business Identity Theft Affidavit, if they suspect their business entity, estate, trust, or exempt organization has been a victim of identity theft.
- (7) BMF ID theft cases will be prioritized and worked expeditiously within established time frames.

#####

25.23.9.2.1
(09-15-2020)
Non-Tax related Identity Theft

- (1) If the taxpayer says they are a victim of ID theft and research determines there is no tax related impact from the theft, guidance will be provided to the taxpayer as to what actions they may want to take.
- (2) If the business has experienced a breach of employee or client data, and the taxpayer is seeking help for their employees or clients, see IRM 25.23.1.6 (1)Data Breach- Business Entities Whose Employees or Clients PII was Breached.
- (3) If the taxpayer has been a victim of a data breach, see IRM 25.23.1.7, Taxpayers who are Victims of a Data Breach. Advise the taxpayer to complete a Form 14039 only for IMF Tax related issues. A Form 14039 is not needed for BMF ID theft.

- (4) If the taxpayer is seeking advice for the business, ask the taxpayer as to the type of information breached:
- If a business or payroll company contacts the IRS to report a data loss which includes 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". In the chart under "Businesses" click on "Form W-2/SSN Data Theft: Information for Business and Payroll Service Providers". This link provides the information on various agencies and how to contact them to report the loss.
 - If a business or payroll company contacts the IRS to report a theft in their office that could potentially lead to a data breach but does not include Form 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 IRS". 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.
 - 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)	https://www.identitytheft.gov	877-438-4338
Social Security Administration (SSA)	www.ssa.gov search "Identity Theft"	800-772-1213

- Advise the caller they may want to contact one of the major credit bureaus. They may be able to help them in obtaining information needed to pursue issues relating to the loss of the business's PII information.

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

- 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, <https://www.naag.org/>
- Provide the taxpayer the [irs.gov](https://www.irs.gov) website advising them to search for "taxpayer guide to identity theft" to obtain more ID theft information.

25.23.9.3
(10-11-2024)

**Business Master File
(BMF) Identity Theft
Liaisons**

- (1) BMF cases can be complex in nature and will at times cross functional lines. All functions have established BMF ID theft liaisons to help in the coordination and working of BMF ID Theft cases. The list of liaisons can be found on the Liaison Contacts Tab on the BMF Identity Theft page. See *Identity Theft BMF Home (irs.gov)*. The liaison contacts can also be found on the SERP Who/Where *Identity Theft - BMF Liaison Contacts - Who/Where - SERP (irs.gov)*.
- (2) BMF ID theft liaisons play an important role in resolving complex cases when the cases cross functional lines.
- (3) The liaisons act as their respective BOD/Function's key point of contact on matters outside the scope of the referring functions or when technical help is needed to either make an ID theft determination or to resolve an ID theft case.
- (4) The liaisons will coordinate with each other to resolve the issue when functions cannot agree about case assignment or resolution.
- (5) Referrals to the functional liaisons are made on Form 14566, BMF Identity Theft Referral. See IRM 25.23.9.8, BMF ID Theft Referrals. Referrals will be liaison to liaison only. All referrals must be sent through the referring function's liaison prior to being sent to another function. The referrals will be sent via secure e-mail to the proper liaison. Follow functional guidelines for referral procedures when forwarding cases to your function's liaison.
- (6) When working paper cases, if the entire case is being transferred, the referring function **WILL NOT** close their case until the receiving functional liaison acknowledges receipt and accepts the case into their function's inventory. This is to prevent cases from being lost in the referral process.

Note: If Form 14039 or Form 14039-B is present, attach the form to the secure e-mail when referring the case.

(7) **The BMF ID theft liaisons will:**

- **When receiving a case referral:**
 1. Review BMF ID theft referral to ensure all required research has been completed and documented on Form 14566, BMF Identity Theft Referral. If the liaison determines the initial research is incomplete or the case does not belong in their inventory, they will reject the referral and return it to the referring liaison within three business days of receipt.
 2. Prior to the referral being accepted, review the case to ensure its completion which includes case documentation. If the case is being referred to be worked or requesting assistance, AMS/CII (if available) will be documented by the referring function with the required information. If the information is not present, reject the referral.
 3. Acknowledge receipt of the referral and advise the referring function the case has been accepted into their inventory within **three** business days and assign to the proper function for resolution. If the referral is for assistance, the receiving function will have **30** days to respond to the assistance request.
 4. If the acceptance or assistance request will take more than 30 days, acknowledge receipt of the referral within **three** business days and provide the referring function with the expected time frame for the response. The case will remain open in the referring function's inventory

until notification that the case is accepted into the receiving function's inventory. If the referral is for assistance, the control will remain open until case is resolved.

- **When referring case to another function:**

1. Review referral to ensure all research has been completed, the control base is still open if appropriate and the case is documented with the required information.
2. Return referral to the employee within three business days if referral is made in error or incomplete.
3. Monitor case for acknowledgement of receipt by the receiving function.
4. If acknowledgement is not received within three business days, send a follow up e-mail to request the status of the determination.
5. Send a follow up e-mail if a response to the assistance referral is not received within 30 days.
6. Return the referral to the employee within three business days when the requested assistance has been provided, the case is accepted, or the referral is rejected.

Note: The Taxpayer Advocate Service (TAS) will use their Operations Assistance Request (OAR) process to direct the OAR to the proper BOD/Function Liaison. TAS OARs should not be sent through the functional liaisons; follow normal functional procedures for processing the OARs. OARs will be reviewed prior to leaving the TAS Organization. As with all BMF ID theft referrals, all required research will be completed before the OAR is sent to the proper liaison. To be considered complete, the OAR must outline all completed research, the facts supporting the ID theft determination and all taxpayer documentation. **Per the SLA: "If the TS Business Unit Liaison/employee determines additional research or documentation is required on an OAR, contact the assigned TAS employee within one (1) workday of the determination, and within one (1) workday of the receipt of the OAR in the case of expedite processing OARs, to obtain information and to negotiate the requested completion date. If the assigned TAS employee cannot provide the information within three (3) workdays of the request, the TS Business Unit Liaison may return the OAR to TAS and the case will be closed out of the unit inventory. TS may provide TAS additional time to obtain the information, where appropriate."**

25.23.9.4
(10-01-2024)
**Business Master File
(BMF) Identity Theft
Research (Inquiry
received via paper or
phones)**

- (1) The required research must be performed once the taxpayer advises you or the employee suspects possible ID theft. This research is to be completed by the employee prior to taking **any** actions on the account, referring the case, transferring the call (this includes accounts in stat 22) or advising the taxpayer to complete a Form 14039-B. The research and determination are vital to ensure the case is placed in the proper ID theft treatment stream as soon as possible. **Never Assume Identity Theft.**

Caution: If a Form 14039-B is received, the case must be moved into the ID theft stream immediately. Once the case is received into BMF IDT, an acknowledgement letter will be sent to the taxpayer within 30 days of receipt. Due to the time frame for sending an acknowledgement letter, a control will be opened by the function receiving the Form 14039-B and the proper ID theft indicators input. See IRM 25.23.9.6, BMF Identity Theft Tracking Indicators. Complete account research will then be completed to determine which function should be handling the case. If the

25.23 Identity Protection and Victim Assistance

case will not remain in the receiving functions inventory, refer the case to the proper function liaison following procedures in IRM 25.23.9.3, BMF Identity Theft Liaisons.

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.

- (2) The depth of the research will be dependent upon the scope of understanding of the employee. This means, if the employee performs in depth IDRS research to perform their job, the same level of research is expected to be performed prior to referring the case to another function's ID theft treatment stream. The employee must research TXMOD/AMDISA to determine if the case originated in Exam function by locating the TC 300 Primary Business Code (PBC). Based on the PBC, the case must be referred to the proper liaison for Field Office or Campus Exam. If the case belongs in the employee's inventory, but some of the research is outside their scope and ID theft is highly probable, the employee will send a referral to the proper liaison to request assistance with researching the case. The case will remain in the referring employee's control and be worked after the research is completed.
- (3) When the inquiry is being handled on the phone, thorough probing must take place to help in determining if ID theft is involved. This includes (this list is not all inclusive):
 - a. Has the business changed to a different type of entity? For example, the business has changed from a sole proprietorship to an LLC. There may be a second EIN, and this may be a case of the returns being filed under an incorrect EIN.
 - b. Has the company changed payroll companies? Many times, if a payroll company has been changed, the old company may still file a return or submit Form W-2.
 - c. If there are payments present, did the taxpayer make any payments? Payment research may provide another EIN or entity information.
 - d. Was the business sold or closed? Was a final return filed?
 - e. If the taxpayer says they never applied for an EIN, has the taxpayer had any ID theft tax related issues under their SSN?
- (4) Perform all required research to rule out a mixed entity (where the inadvertent use of one taxpayer's TIN is used to file another taxpayer's return) or successor corporation, and to locate any possible cross-reference TIN. Refer to Exhibit 25.23.9-7, BMF Identity Theft Research requirement to help you with case building. The required research must be performed to help in making an ID theft determination. Research should include (this list is not all inclusive):
 - a. All related IMF and BMF accounts. Research the EIN (both the Entity and TXMOD/BMFOL) and look for any cross-reference SSN or other business relationships. Research using CC NAME, FINDE for a business with a similar name at a different address, etc. to determine if there was a mixed entity or successor corporation. When the IRS establishes an EIN, BMFOLE should reflect an XREF SSN/ITIN for the individual or entity requesting the EIN assignment. Preliminary research will include reviewing all cross-reference ITINs, and SSNs.

- b. Research any payments to help in determining if the return in question

#

on the account. Follow functional procedures to determine if payment needs to be moved to another account or to excess.

- c. Review the returns via on-line resources prior to ordering the documents. Conduct research of all returns involved using CC TRDBV or MeF. If unable to review the needed documents on-line, request the document using CC ESTAB. It may contain information needed to determine if ID theft exists. Follow functional procedures when requesting a document from files. Search returns, schedules, forms and attachments. Review and compare the following with information provided by the taxpayer.

Note: If research deems mixed entity and not IDT follow your normal functional procedures to resolve the taxpayer's issue.

#

- d. Use CC IRPTRI to view any Forms W-2 and all related income documents filed under the EIN. If there were income documents filed under the EIN, it may be necessary to review the IMF accounts associated with these documents. If there are fraudulent returns filed under these SSNs, it may help with the BMF ID theft determination.

Example: The taxpayer stated the business changed entities and new EIN was issued. No returns should be filed for the old number and the taxpayer suspects ID theft. Research shows returns were filed for the last quarter and CC IRPTRI shows Forms W-2 filed. Research of the IMF accounts shows duplicate Forms W-2 were filed for each employee, one under each EIN. This is probably not ID theft, but an internal error made by the company or payroll company.

- e. Review all case history such as AMS/CII to review all prior contacts made by the taxpayer.

#

- g. Consult your functional IRM for more research requirements when working ID theft cases.
h. Carefully review any documentation the taxpayer has provided in support of their claim.

- (5) Upon receipt/assignment of an identity theft case, an initial cursory review must be performed to identify all taxpayer issues. Identifying issues at the beginning of the case provides a higher level of customer service and reduces the potential for unresolved problems.

Reminder: If there is an unpaid balance due, suspend collection and notice activity until the identity theft issue is resolved. Refer to functional IRMs for additional guidance.

- (6) If after all research is completed and it is determined ID theft does not exist, follow normal procedures for handling the account.
- (7) If the employee has AMS or CII access, document AMS/CII with all related information. This documentation is to include the research completed, the information supporting the ID theft determination, if and where a Form 14566 is sent and closing actions.

Reminder: If Form 14039 or Form 14039-B is present, attach the form to the secure e-mail when referring the case.

25.23.9.4.1
(10-01-2025)
**BMF Returns Selected
for Return Integrity and
Compliance Services
(RICS) Review**

#

#

#

will cause the return to post as a TC 973 instead of a TC 150.

#####

Note: A TC 971 AC 123 may be on the account with a miscellaneous code BMF IDT RP after an IDT determination has been made. The TC 971 AC 123 is to notify employees that the account was deemed IDT and was worked in a bulk process. This action code does not change any actions that should be taken regarding the IDT issue.

- (4) There will be an open control assigned to 1481055555, with a category code of BIDT and an activity code showing showing potential IDT (POTENTIDT). If a paper case is received that meets the criteria above Accounts Management employees use IRM 25.23.11.6.3, BMF Returns Selected for RICS Review. All other employees follow your business unit's functional procedures.
- (5) For returns selected under a RICS BMF program, RICS sends Letter 6042C, Entity Verification for Businesses, to verify the business entity. If there is an X-REF SSN showing on CC BMFOLE, a letter will also be sent to the X-REF. If there is no X-REF, the letter will only be sent to the address shown for the business.
- (6) If a TC 971 AC 711 posts, that return is suspended. The TC 971 AC 711 will cause the return to post as a TC 973, and it will remain suspended until the taxpayer validates the return. The TC 971 AC 711 can be generated by:
 - a. The return being caught in a filter or
 - b. The return contains a Computer Condition code (CCC) of E
- (7) The TC 973 return will be suspended for up to three years from the TC 973 posted cycle. If the return is not validated within that three-years, it will be deleted from the suspense file.

Note: Three-year suspension period is 156 cycles (weeks) from the cycle the TC 973 posted in .

- (8) 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.
- (9) If RICS determines that the selected return is not IDT, RICS will take appropriate account actions. If a TC 971 AC 711 posted suspending the return, a TC 971 AC 712 with corresponding DLN of the TC 973 is input allowing that return to post. If a TC 971 AC 522 posts indicating return selected, RICS will reverse as applicable.
- (10) If RICS determines that the selected return is not IDT but there are questionable Frivolous or fraudulent items, RICS will take appropriate account actions to refer the case to either FRP or SBSE for further review. If a TC 971 AC 522 indicating return selected is present, RICS will reverse as applicable and notate case referred to other area for review.
 - If referring to FRP, and a TC 971 AC 711 posted suspending the return, a TC 971 AC 713 with corresponding DLN of the TC 973 is input allowing that return to post and freeze any refund with a TC 810 (-Q freeze) RC 4.

25.23 Identity Protection and Victim Assistance

- If referring to SBSE, and a TC 971 AC 711 posted suspending the return, a TC 971 AC 717 with corresponding DLN of the TC 973 is input allowing that return to post and freeze any refund with a TC 810 (-Q freeze) RC 8
- (11) If a TC 971 AC 711 post suspending the return and the return was deleted from the suspense file, RICS will reverse the TC 971 AC 711 if they determine it is not IDT and:
- a. If the return was electronically submitted, the EUP return will be printed and sent to be processed as paper using the original receive date.
 - b. If the return was paper, the paper return will be secured and sent for processing using the original received date.

Reminder: In both situations, the original DLN will be crossed out on the return for processing to assign a new DLN.

Example: 1. Return is identified as a potential IDT case. RICS issues letter and suspends their case pending a response. No reply to letter is received. RICS closes potential IDT case as no reply. Three years later there still has not been a reply from the business.

1. Return was selected by filters and a TC 971 AC 711 is generated on the account.
2. BMF sees the TC 971 AC 711 and posts the return as a TC 973. The return is placed into suspense on the SCRS (Service Center Replacement System) for three years.
3. Taxpayer doesn't respond to the letter sent.
4. Three years after the TC 973 posted cycle, the return is deleted from the suspense file.

Example: 2. Return is identified as a potential IDT case. RICS issues letter and suspends their case pending a response. No reply to letter is received. RICS closes potential IDT case as no reply. Business replies passing authentication and verifies return filing 25 months after TC 973 posted to the account. Further classification of the return shows no auditable items that would require the refund to be held.

1. Return was selected by filters and a TC 971 AC 711 is generated on the account.
 2. BMF sees the TC 971 AC 711 and posts the return as a TC 973. The return is placed in suspense on SCRS.
 3. Taxpayer validates the return within three years from the TC 973 posted cycle and a TC 971 AC 712 is input with the DLN of the TC 973 it is reversing.
 4. Return posts as the TC 150 and refund released.
- (12) If the taxpayer calls about a notice requesting a return to be filed but original return is being held for RICS review or letter pending RICS review, then Accounts Management employees will follow IRM 25.23.11.6.3 , BMF Returns Selected for RICS Review. All other employees follow your business unit's functional procedures.

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

25.23.9.4.2
(10-01-2024)

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

- (1) Identity thieves sometimes use the personally identifiable information (PII) of individuals to establish fabricated businesses. Many times, the fabricated business is used to support the filing of fraudulent IMF returns.
- (2) If the taxpayer calls advising they received correspondence relating to a BMF ID theft issue and claims to have no affiliation with the business, take the proper steps to ensure ID theft has occurred. DO NOT advise the caller to submit a Form 14039 on any IMF or BMF toll free line claiming possible BMF ID theft.
- (3) If the taxpayer does file a Form 14039 to advise the IRS of ID theft relating to a business/BMF issue, the receiving BMF CSR will send the proper acknowledgment letter.
- (4) Employees will verify the IMF taxpayer's association with the EIN and determine if potential BMF ID theft exists prior to marking the IMF account with a tracking indicator.

Example: Jane Smith calls an IMF related toll-free line to report she believes her personal identity has been stolen. She received an IRS notice demanding payment for unpaid employment taxes on Janes' Flowers located in Florida (Jane lives in the Northwest). Jane has never owned a business and never resided in Florida. Jane provides the CSR with her SSN and the EIN on the notice.

- (5) Research MUST be completed to determine if there is a potential BMF ID theft issue prior to marking an account and referring or transferring the case/call to another area. Researching the account will allow for the employee to determine if the case should be referred to the BMF ID theft inventory or moved/transferred into the regular BMF inventory following normal procedures.
 - a. Research CC BMFOLE (the business entity module) to determine if the taxpayer's SSN is associated with the EIN. BMFOLE contains a XREF-SSN field that will provide the associated SSN. The format for CC BMFOLE is:
BMFOLEX-XXXXXXX.

#

Caution: Individual taxpayers reporting to be victims of a Business-related identity theft should file Form 14039-B, Identity Theft Affidavit, and provide an explanation in section D.

- (6) Once the research is completed and it is determined there is potential ID theft, research CC IMFOLE to determine if there is an existing TC 971 AC 504

25.23 Identity Protection and Victim Assistance

SPCL2. If there is currently no ID TC 971 AC 504 SPCL2 marker, the SSN entity must be marked on CC ENMOD using CC REQ77 as shown in IRM 25.23.2.8.1.2, TC 971 AC 504 - Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, and EAFail, for more information. Input the XREF EIN in the XREF-TIN section on the REQ77 to post with the TC 971 AC 504.

- (7) Potential identity theft case needs to be referred to the proper BMF ID theft Liaison. The following will help in determining to which liaison the referral should be sent.
 - ◆ CAWR assessment- CC TXMOD will show a TC 290 assessment in blocking series 55
 - ◆ Exam assessment- CC TXMOD will show a TC 300 assessment or open Exam freeze (-L). Identify the PBC code and refer to the proper Field or Campus Exam liaison.
 - ◆ 6020b assessment- CC TXMOD will show the literal "6020b" at the end of the TC 150 assessment and RCC "4"
 - ◆ SFR assessment- CC TXMOD will show the literal "SFR" at the end of the TC 150 assessment.
 - ◆ Field Exam- CC AMDISA will show Primary Business Code (PBC) See *Exam Employee Group Code (EGC) Contacts*. Click on the Employee Group Code (EGC) listing Contacts to see who is working on the case based on the PBC code.
 - ◆ Field collections- CC TXMOD will show service center status 26
 - ◆ ACS- CC TXMOD will show service center status 22
 - ◆ Accounts Management- Any case that does not meet other account criteria
 - ◆ Criminal Investigation (CI) – If associated tax period or entity is controlled to CI with an un-reversed Transaction Code (TC) of 914, 916, or 918.
- (8) Send Form 14566, BMF ID Theft Referral via secure e-mail to the proper BMF ID Theft Liaison. The listing is found on the *Identity Theft-BMF Liaison Contacts* page. In the explanation section on Form 14566, include any actions that you input on the SSN. Do not hold cases for completion; link CII cases to expedite processing. For more information, see the referral procedures in IRM 25.23.9.3, BMF ID Theft Liaisons. Document AMS/CII, if available, to reflect the referral sent, advise if the Form 14039 was submitted, the suspicious EIN and where the referral is being sent.

Example: Referral emailed to the BMF ID theft CAWR Liaison, the history would read:

TP submitted Form 14039 under SSN. TP states no involvement with EIN XX-XXXXXXX. (Include any other information considered important.)

- (9) If there is no indication of potential BMF identity theft and there is a TC 971 AC 504 on the account, reverse with a TC 972 AC 504 SPCL2. Refer to IRM Exhibit 25.23.2-5, IMF Only TC 972 AC 504 - Reversal of TC 971 AC 504. Route the case per normal procedures.

25.23.9.5
(10-01-2022)

Identity Theft Case Building- Business Master File (BMF)

- (1) Once BMF ID theft is either confirmed or it is determined there is a high probability of ID theft, the case will be moved into the ID theft treatment stream. All information provided by the taxpayer and research completed should be documented on the case (AMS/CII if available).
- (2) Once the case is placed into the ID theft treatment stream, an IDRS control must be opened and the ID theft indicator input. See IRM 25.23.9.5.1, Control-

ling BMF ID Theft Cases, and IRM 25.23.9.6, BMF Identity Theft Tracking Indicators.

Exception: If a Form 14039-B is received the case must be moved into the ID theft stream immediately. Once the case is received into BMF IDT, an acknowledgement letter will be sent to the taxpayer within 30 days of receipt. Due to the time frame for sending an acknowledgement letter, a control will be opened by the receiving function, the proper ID theft indicators input and the Letter 5316C sent. See IRM 25.23.9.6 BMF Identity Theft Tracking Indicators. Employees must complete account research to determine which function should be handling the case. If the case will not remain in the receiving functions inventory, refer the case to the proper function liaison following procedures in IRM 25.23.9.3, BMF Identity Theft Liaisons.

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) When working the ID theft case, if the information provided by the taxpayer tends to show the potential for ID theft but more information is needed, the taxpayer may need to complete the Form 14039-B, Business Identity Theft Affidavit. Refer to IRM 25.23.9.7 Form 14039-B, Business Identity Theft Affidavit. If this form is needed to validate a claim of identity theft, you can send the form to the taxpayer or request they download it from [irs.gov](https://www.irs.gov).
- (4) Employees working phones can advise the taxpayer to complete the Form 14039-B, BMF Identity Theft Affidavit, unless there is an open control and the case is being worked in their function. If there is an open control to another function, send a referral to that function's ID theft liaison documenting the taxpayer's explanation and completed research supporting their claim of ID theft. If there is no open control and the employee has completed the required research and the potential for ID theft exists, request the taxpayer file Form 14039-B, Business Identity Theft Affidavit.
- (5) If the case is being retained in your function but assistance is needed in resolving the case, a referral for assistance can be requested. The case will remain open while assistance is being requested. See IRM 25.23.9.8, BMF Identity Theft Referrals.
- (6) Identity theft often leaves its victims feeling helpless and distraught. IRS employees should exercise empathy in dealing with victims.
- (7) Identity theft cases will be prioritized and worked expeditiously and within established time frames.

25.23.9.5.1
(10-01-2025)
**Controlling Business
Master File (BMF)
Identity Theft Cases**

- (1) Once ID theft or the possibility of identity theft has been confirmed, the case must be moved into the proper ID theft treatment stream and a control base must be opened if the employee has access to IDRS. The control base will remain open until **ALL** case issues have been resolved. If the case is originally in your function's inventory but is being referred to another to be worked, the control will remain open until the case is accepted by the receiving function's liaison. Refer the case following functional guidelines for referral procedures.

25.23 Identity Protection and Victim Assistance

- (2) If the contact is by phone and the case is being referred into another function's ID theft treatment stream, the function receiving the case will open the control when the case is accepted into their inventory. Annotate on the referral "phone contact". If your function is keeping the case, open the control based on functional guidelines.
- (3) The responsible function (Collections, Examination, CAWR, FUTA, AM, etc.) will keep control from receipt to closure. All required account actions will be coordinated through the function with the open control.
- (4) If more information is needed, the controlling function will send the Form 14039-B to the taxpayer and suspend the case. See IRM 25.23.9.7, Form 14039-B Business Identity Theft Affidavit.
- (5) Accounts affected by BMF identity theft are often complex and cross functional lines. When this occurs, the controlling function will refer that part of the case needing action by another function. The Form 14566, BMF Identity Theft Referral was developed for this purpose. Refer to IRM 25.23.9.8, BMF Identity Theft Referrals for more information. The responsible function will put their IDRS control into "B" status to designate the case as suspended pending the referral completion.
- (6) The controlling function is responsible for:

- Issuing the required correspondence.
1- Acknowledgment letter- When an ID theft claim is received from the taxpayer, it must be acknowledged by sending a Letter 5316C, BMF Identity Theft Documentation Acknowledgment and Interim Letter (Form 14039-B and supporting documentation) within 30 days of 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.

Exception: If a Form 14039-B is received and there is no active ID theft case open, the case will be controlled by the receiving function and a Letter 5316C sent to acknowledge receipt of the form and the ID theft indicator input. Once completed, the account should be researched to determine if the case should remain in the receiving inventory or referred to another functional liaison. If the case is being referred, the control will remain open until referral is accepted by that function.

2- Interim if required. Send Letter 5317C, BMF Identity Theft Request for Information or Closing Letter.

3- Closing letter- Send Letter 5317C BMF Identity Theft Request for Information or Closing Letter when ID theft issue has been resolved.

- Suspend collection activity, as appropriate.
- Input of the BMF ID theft indicator, TC 971 AC 522 IDTCLM. If a Form 14039-B is received, input the follow up indicator TC 971 AC 522 IDTDOC. See IRM 25.23.9.6, **BMF Identity Theft Tracking Indicators**

- Complete research if needed or send Form 14039-B to the taxpayer for completion.

Note: This list is not all inclusive.

- (7) The function working the ID theft case, will ensure all issues are resolved and adjustments are posted prior to case closure. Input the closing TC 971 AC 522. Refer to IRM 25.23.9.6, BMF Identity Theft Tracking Indicators, for more information.

25.23.9.5.2
(09-15-2020)
**Tracking Business
Master File (BMF)
Tax-Related Identity
Theft Inventory**

- (1) In situations where the taxpayer makes an allegation of identity theft or when the IRS initially suspects that identity theft may have occurred, and preliminary research has been completed, the IRS controlling function will apply an identity theft indicator. The identity theft tracking indicator alerts others that a claim of identity theft has been reported and provides the IRS with a method to quantify the scope of BMF Identity Theft. Refer to IRM 25.23.9.6, BMF Identity Theft Tracking Indicators, for more information.

Caution: BMF identity theft indicators (unlike some of those used on IMF accounts) do NOT systemically generate any systemic notices to the taxpayer. All taxpayer notifications are manual.

- (2) In most instances, for taxpayer-initiated claims of identity theft, the case MUST be moved into identity theft inventory once the taxpayer has provided Form 14039-B to support a claim of identity theft. This provides victims with a treatment stream for case resolution specific to identity theft. For more information about identity theft documentation, refer to IRM 25.23.9.7, Form 14039-B, BMF Identity Theft Affidavit and IRM 25.23.9.6.2 , Taxpayer Supporting Documentation - TC 971 AC 522 IDTDOC.
- (3) If after the account has been marked with a BMF Identity Theft Indicator, the employee determines identity theft did not occur, the BMF ID theft tracking indicator will be reversed by the employee assigned. This removes the case from identity theft inventory. See Exhibit 25.23.9-5, Reversing BMF Identity Theft Indicators, for more information. All other non-identity theft issues will be resolved using normal procedures.

25.23.9.6
(10-01-2025)
**Business Master File
(BMF) Identity Theft
Tracking Indicators**

- (1) BMF identity theft indicators are applied in situations where the taxpayer makes an allegation of ID theft or when the IRS initially suspects that identity theft may have occurred. In both scenarios, IRS functions will apply an identity theft indicator. The identity theft tracking indicator alerts others that a claim of identity theft has been reported. Each BMF ID Theft indicator is input as a Transaction Code (TC) 971 with Action Code (AC) 522 using Command Code REQ77 on the **TXMOD** of all accounts affected by identity theft.
- (2) Review the accounts for prior ID theft indicators before inputting the initial TC 971 AC 522. Use IDRS CC TXMODA or BMFOLT to view the posted transactions. **If the account is already marked with a TC 971 AC 522 IDTCLM, do not input a second code for the same MFT and Tax period even if the initial TC 971 AC 522 IDTCLM reflects another BOD/Program.**
- (3) BMF Identity theft tracking indicators, unlike those used for IMF, are applied to all MFTs and Tax Periods affected by identity theft. IPSO established distinctive Tax Administration Source Codes for BMF accounts.

Action Code	Tax Administration Code	Definition
522	IDTCLM	Taxpayer makes a claim of identity theft, but no taxpayer documentation provided, refer to IRM 25.23.9.6.1, Allegation or Suspicion of BMF Identity Theft - TC 971 AC 522 IDTCLM, for more information. Taxpayer may still need to complete Form 14039-B. Also input when there is IRS identified BMF identity theft.
522	IDTDOC	Taxpayer provided a Form 14039, Form 14039-B or Taxpayer Supporting Documentation. See <i>IRM</i> 25.23.9.6.2, Taxpayer Supporting Documentation - TC 971 AC 522 IDTDOC for more information. 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. Refer to IRM 25.23.9.6.3, Closing BMF Identity Theft Issues - TC 971 AC 522 CLSIDT, for more information.
524	EINFAB	EIN is fabricated and the account has been locked. This TC 971 can only be input by IP and RICS
524	ENTLOK	Applied to a legitimate entity when identity theft is confirmed, and the entity is locked to prevent name, address, and responsible party updates. This TC 971 can only be input by IP and RICS

- (4) If after the account has been marked with a BMF Identity Theft Indicator, the employee determines identity theft did not occur, the BMF ID theft tracking indicator will be reversed by the employee assigned. This removes the case from identity theft inventory. See Exhibit 25.23.9-5, Reversing BMF Identity Theft Indicators - TC 972 AC 522, for more information. All other non-identity theft issues will be resolved using normal procedures.
- (5) If the EIN account has been locked by TC 971 AC 524 posting, this will be visible on CC BMFOLE. 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.

25.23.9.6.1
(10-01-2025)
**Allegation or Suspicion
of Business Master File
(BMF) Identity Theft
Transaction Code (TC)
971 Action Code (AC)
522 IDTCLM**

- (1) Prior to marking a taxpayer's account with a BMF identity theft indicator, all required preliminary research **must be completed** to rule out a possible mixed entity and the case **MUST** be assigned and controlled. Refer to IRM 25.23.9.4, BMF Identity Theft Research (Inquiry received via paper or phones) for more information.

Reminder: The BMF indicator is to be input by the function working the case. If you **are not** keeping control of the case, **do not** input the TC 971 AC 522.

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.

- (2) Place an identity theft indicator on all MFTs and tax periods affected to ensure the account is moved into ID theft treatment stream. The identity theft indicator is input on taxpayer asserted BMF identity theft accounts and the IRS identified BMF identity theft cases.
- (3) If the contact is by phone and the case is going to be kept in your inventory, open the control and input the TC 971 AC 522 based on functional IRM guidance.
- (4) To mark the taxpayer's account involving BMF identity theft, use Command Code (CC) REQ77 initiated from TXMOD to input a TC 971 AC 522 IDTCLM with the Tax Administration Code designated for your function. Refer to Exhibit 25.23.9-1, TC 971 AC 5XX - MISC Codes. The BMF indicators work differently from IMF indicators. Ensure the secondary date and "MISC" sections are correctly input.
 - **The Secondary Date** field will reflect the **IRS received date** of the taxpayer's inquiry or **the date of the call**. If the identity theft issue was internally identified, use the date you recognized the taxpayer was a victim of identity theft. Exception: RICS systemic selections for potential BMF IDT review do not contain a secondary date.
 - **The MISC>** field will reflect your BOD and Program name as shown in Exhibit 25.23.9-1, TC 971 AC 5XX - MISC Codes and Exhibit 25.23.9-2, BMF ID Theft Indicators - TC 971 AC 522 IDTCLM - Initial Allegation or Suspicion of BMF ID Theft.

Caution: If the account is already flagged with a TC 971 AC 522 IDTCLM, do not input a second code for the same MFT and Tax Period even if the initial TC 971 AC 522 IDTCLM reflects another BOD/Program.

- (5) Taxpayer identified BMF identity theft claims will be researched by the receiving function. If after all the required research is completed, it is determined there is a potential ID theft and the case is outside the scope of your function, refer the case to the proper liaison but do not input the TC 971 AC 522. The receiving function will control the case and input the TC 971 AC 522. If the receiving function is keeping the case, open the control and input the TC 971 AC 522 based on functional guidelines. Internally identified BMF identity theft accounts will be controlled and the TC 971 AC 522 input by the initiating function using date when preliminary research was completed. Refer to your functional IRM for information about account controls.

Note: Because of the high probability of mixed entity, employees **MUST** perform research to rule out a mixed entity or other non-identity theft related situation. Refer to IRM 25.23.9.4, BMF Identity Theft Research (inquiry received via paper or phones) , for more information.

- (6) Once it is determined the case will remain in your inventory:

If	And	Then
After all preliminary research is completed and you are unable to verify that BMF ID theft has occurred IRM 25.23.9.4 BMF Identity Theft Research	additional information is needed to verify ID theft	<ol style="list-style-type: none"> 1. Control and assign the case to ID theft inventory 2. Send the taxpayer a Form 14039-B and request a response in 30 days 3. Suspend any collection activity 4. Input TC 971 AC 522 IDTCLM on the affected tax periods and MFTs. 5. If the taxpayer does not respond, reverse the ID theft marker with a TC 972 AC 522 NORPLY, close the case, release collection holds and work any remaining issues using your normal procedures <p>Note: Provide an additional 15 days for responses from entities with foreign addresses.</p>

If	And	Then
After all preliminary research is completed and you are unable to verify that BMF ID theft has occurred	You have performed all preliminary research as required and the case is NOT within functions scope IRM 25.23.9.4 BMF Identity Theft Research	<ol style="list-style-type: none"> 1. Complete Form 14566 BMF Identity Theft Referral and forward to your ID theft liaison for review following functional guidelines. If case is controlled leave control open until the referral is accepted. 2. The function receiving the case will open a control, input the TC 971 AC 522 and send the Form 14039-B if appropriate.

- (7) If the employee later determines identity theft did not occur, the BMF ID theft tracking indicator will be reversed by the employee assigned. This removes the case from identity theft inventory. All other non-identity theft issues will be resolved using normal procedures. See Exhibit 25.23.9-5 Reversing BMF Identity Theft Indicators, for more information.

25.23.9.6.2
(09-15-2020)
Taxpayer Supporting Documentation - Transaction Code (TC) 971 Action Code (AC) 522 IDTDOC

- (1) This code will only be applied to accounts when the IRS receives a completed Form 14039, Identity Theft Affidavit or Form 14039-B, Business Identity Theft Affidavit, from the taxpayer. Refer to IRM 25.23.9.7, Form 14039-B, Business Identity Theft Affidavit, for specific information about this form.
- (2) After verifying the Form 14039 or Form 14039-B and associated taxpayer documents are complete and legible, you will need to mark the taxpayer's account to reflect IRS receipt.
- (3) From TXMOD, you will use Command Code (CC) REQ77 to input a TC 971 AC 522.
The Secondary Date: field will reflect the **IRS received date** of the taxpayer's documents
The MISC>: field will be input to reflect your BOD and Program.
Refer to Exhibit 25.23.9-1 TC 971 AC 5XX - MISC Codes and Exhibit 25.23.9-3 BMF ID Theft Indicators - TC 971 AC 522 IDTDOC - BMF ID Theft Documentation for more information.

25.23.9.6.3
(11-06-2020)
Closing Business Master File (BMF) Identity Theft Issues- Transaction Code (TC) 971 Action Code (AC) 522 CLSIDT

- (1) **Case Closure Analysis:** The input of the TC 971 AC 522 CLSIDT signifies there was ID theft and all account actions have been completed and the case closed. If it was determined that no ID theft has occurred, you must reverse the TC 971 AC 522. See IRM 25.23.9.6.5, Reversing BMF Identity Theft Indicators, for more information. Perform case closure analysis to ensure all identity theft related issues have been addressed and resolved. This includes but is not limited to:
 - Review both prior (a minimum of three prior years) and subsequent years for apparent evidence of unresolved identity theft issues
 - Release notice or enforcement holds as appropriate
 - Ensure the victim received their proper refund if one is due
 - Verify and update the taxpayer's address

- Close down fabricated EIN
- If the EIN is not active, delete filing requirements
- Move payments not belonging to the taxpayer based on functional guidelines. If out of scope, refer to the proper area to have the payment moved. Do not close the case until all actions have been taken by assisting function.
- Take all required account actions
- Send closing letter to taxpayer

Reminder: If it is determined ID theft does not exist, the TC 971 AC 522 must be reversed not closed. See IRM 25.23.9.6.5, Reversing BMF Identity Theft Indicators

- (2) Other outstanding account issues identified during case closure analysis should ONLY be referred to another function when the case cannot be resolved within your function.
- (3) The employee assigned the case will close the identity theft issue by marking the account with a TC 971 AC 522 with the Tax Administration Source Code for their BOD and Program. Refer to IRM 25.23.9.6, BMF Identity Theft Tracking Indicators.

Note: Refer to Exhibit 25.23.9-4 BMF ID Theft Indicators - TC 971 AC 522 CLSIDT - Close and Confirmed as BMF ID Theft for more information.

25.23.9.6.4
(05-09-2022)

**Locking Accounts-
Transaction Code (TC)
971 Action Code (AC)
524**

- (1) We currently have the capability to lock accounts. An account can be locked in the following situations:
 - A Fabricated EIN
 - A Business no longer has any federal filing requirements
 - A business is closed
 - A business is no longer operational (defunct)
 - A business has been inactive for 3 or more years
 - A business filed final returns
- (2) If ID theft has been determined and the taxpayer says they have no association with the business, the account can be locked to prevent the filing of any returns or allow for the usage of the EIN on any IMF filings. IRM 25.23.9.8.1, Fabricated or Inactive EIN Procedures, for working these cases.
- (3) In situations where the taxpayer has stated the business is closed and the EIN has been used to either file fraudulent BMF filings or income documents, the account can be locked. In these situations, you will need to send a referral to IP to have the account locked. Follow the procedures in IRM 25.23.9.8.4, Referrals to Lock the Account.
- (4) Accounts will only be locked in situations where there is confirmed ID theft, business is closed, inactive, or the EIN has been considered fabricated.
- (5) If the account has been locked in error, send a referral following the procedures in IRM 25.23.9.8.4, Referrals to Lock the Account, and request the lock be reversed.

25.23.9.6.5
(01-03-2020)

Reversing Business Master File (BMF) Identity Theft Indicators

- (1) BMF identity theft reversal codes provide better tracking of alleged BMF ID theft cases. If it has been determined that there is no ID theft on the account and there is a TC 971 AC 522 on the module, **you must** reverse the indicator. The table below provides a listing of the codes used when reversing a BMF identity theft allegation. It is imperative that the BMF identity theft indicators are reversed when BMF identity theft did NOT occur or was not substantiated by the taxpayer. This is to remove the case from the identity theft population. If reversing the indicator, you must annotate AMS/CII with the information that supports the reversal.

Reason for BMF ID Theft Reversal	Reversal Code
If, after completing a case analysis, you have determined ID Theft did not occur. Example: The taxpayer contacts the IRS believing to be a victim of identity theft. After careful case analysis and review, the employee determines this is a mixed entity case, no identity theft occurred.	NOIDT- Document on AMS/CII why it is determined no ID Theft.
The taxpayer did not respond to your request for supporting documentation and you cannot make a determination of identity theft using internal resources.	NORPLY
The BMF ID Theft indicator was applied due to a typographical mistake or another internal mistake.	IRSERR
The original identity theft incident claim was determined to be fraudulent.	FALSE
The reason for the 971 reversal does not meet any of the above reason descriptions.	OTHER- Document on AMS/CII the reason for the reversal.

25.23.9.6.6
(01-03-2020)

Reversing Business Master File (BMF) Identity Theft Indicators - Transaction Code (TC) 972 Action Code (AC) 522 NORPLY

- (1) An account will be marked with a TC 972 AC 522 NORPLY when a request was made to a taxpayer to submit more information to support the identity theft claim and no taxpayer response was received. This request for more information is issued when the determination cannot be made based on internal research.
- (2) Use Command Code (CC) REQ77 initiated from TXMODA to input a TC 972 AC 522 reflecting a Tax Administration Source Code NORPLY in the "MISC" field. Refer to Exhibit 25.23.9-5, for more information.
- (3) If the taxpayer contacts the IRS after the TC 971 AC 522 is reversed due to a no reply, a new TC 971 AC 522 IDTCLM needs to be input using the secondary date of the original TC 971 AC 522.

25.23.9.6.7
(09-04-2015)

**Reversing Business
Master File (BMF)
Identity Theft Indicators
- Transaction Code (TC)
972 Action Code (AC)
522 NOIDT**

- (1) In situations where it is determined no identity theft occurred, a reversal of the BMF identity theft indicators present on the tax module(s) must be completed. Document on AMS/CII the reasoning behind the determination that no ID theft exists.

Example: The taxpayer receives a balance due notice from the IRS and suspects identity theft. After performing the required research, you determine the balance due was not a result of identity theft but rather a result of a return processed to an incorrect account. This is not identity theft.
- (2) Use Command Code (CC) REQ77 initiated from TXMODA to input a TC 972 AC 522 reflecting a Tax Administration Source Code NOIDT in the "MISC" field. Refer to Exhibit 25.23.9-5, for more information.

25.23.9.7
(10-01-2025)

**Form 14039-B, Business
Identity Theft Affidavit**

- (1) Form 14039-B, Business Identity Theft Affidavit, is used for a business to file an ID Theft claim. Prior to August 1, 2020, this form was an internal form sent to the taxpayer by the IRS to gather taxpayer information vital to making an identity theft determination.
- (2) Form 14039-B supporting documentation consists of the following items:
 - a. **Sole Proprietor** - a passport, driver's license or a valid U.S. federal or state government issued form of identification with a signature and a copy of a utility bill, invoice, mortgage/rent receipt or other documentation to support business operations.
 - b. **Corporations, Partnerships, Limited Liability Company, Exempt Organizations, Estate or Trust** - one of the following: Articles of incorporation, Articles of organization, Trust or Estate document, a statement signed by an officer or director on corporate letterhead stationery stating that the person who signed Form 14039-B has authority to legally bind the company.

Note: If the claimant did not request an EIN and has no knowledge of the EIN, they will not need to provide evidence of business operations.
- (3) If the taxpayer does not provide supporting documentation within the requested time period and you cannot make a determination about BMF ID theft, you will close the identity theft issue by reversing the BMF Identity Theft Indicator and proceed with normal case resolution assuming the taxpayer is not an identity theft victim. Refer to Exhibit 25.23.9-5 Reversing BMF Identity Theft Indicators.

Reminder: If the taxpayer does not respond to the request for information and you are closing the identity theft issue, you **MUST** reverse the BMF Identity Theft Indicators.

- (4) Form 14039-B must be signed by the taxpayer or someone who has a valid power of attorney for the taxpayer, (e.g., Form 2848, Power of Attorney and Declaration of Representative.
- (5) Documents must be secured and handled in the same manner as other sensitive taxpayer information. The documents must be retained and filed with the resolved case.
- (6) The business unit/function that is assigned the identity theft case (relevant open control) or issued the notice/letter relating to the identity theft (CP 504

Balance Due Notice, Audit Notice, etc.) is responsible for collecting supporting documentation in a timely, accurate, and secure manner.

- (7) After the receipt of the taxpayer's documentation, you will need to research the case to verify the taxpayer's claim. If it is later determined that identity theft did not occur, reverse the TC 971 AC 522, refer to IRM 25.23.9.6.5, Reversing BMF Identity Theft Indicators.
- (8) If a Form 14039-B is received an acknowledgement letter must be sent to the taxpayer to verify receipt within 30 days.

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.

If the case is not already controlled to an ID theft treatment stream, the receiving function will send the acknowledgement letter, open the control and input the TC 971 AC 522. If the case is being transferred to another function's inventory, the case control will remain open until the acceptance by that function is received. If there is an open control in another function's ID theft treatment stream, refer the form to the proper function. They will send the letter and input the TC 971 AC 522.

Caution: Receipt of documentation from the taxpayer does not validate an identity theft claim. Proper research **MUST** be performed prior to reaching an identity theft determination.

- (9) If you have completed preliminary research and ruled out mixed entity but are unable to determine if BMF identity theft occurred, print and mail Form 14039-B to the taxpayer.

If the taxpayer alleges identity theft	And	Then request the taxpayer complete form 14039-B and provide the following
Claims to have no knowledge of applying for an EIN	there is a possibility ID theft exists	A clear copy of one of the following documents: <ul style="list-style-type: none"> • Valid state issued driver's license • Valid passport • Other valid U.S. Federal or State government issued identification (For example, Visa)

If the taxpayer alleges identity theft	And	Then request the taxpayer complete form 14039-B and provide the following
Has an active or inactive sole proprietorship	there is a possibility ID theft exists	<p>A clear copy of one of the following documents:</p> <ul style="list-style-type: none"> Valid state issued driver's license Valid passport Other valid U.S. Federal or State government issued identification (For example, Visa) <p>AND if the taxpayer is an active sole proprietorship, the taxpayer must provide a clear copy of one of the following documents:</p> <ul style="list-style-type: none"> Utility bill Mortgage/Rent Statement Other documentation to support business operations
Has an active or inactive Corporation, Partnership LLC, Exempt Organization, or Trust	there is a possibility ID theft exists	<p>One document from the list below and a copy of CP 575 Notice of EIN Assignment, if the claimant has a copy available.</p> <ul style="list-style-type: none"> Articles of incorporation A written statement by the officer or director on corporate letterhead stationery, to the effect that he/she has authority to legally bind the corporation Articles of organization Trust or estate document

25.23.9.7.1
(05-09-2022)

Complete and Legible Documents

- (1) When a taxpayer submits Form 14039-B, the Form 14039-B and associated document(s) must be reviewed to determine if they are legible and complete.
- (2) A document is considered legible when the copies provided are clear and easily read. Once you have determined the documentation provided is complete and legible, initiate taxpayer contact to notify the taxpayer the information requested has been received.

Caution: Acknowledgement of receipt of the Form 14039-B is required within 30 days of receipt unless the document is received face to face.

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) When the documentation is NOT legible/complete:

Note: If the documentation provided is not complete or legible but you can make a determination using internal research, resolve the identity theft issue. Do not request the documents again. Once all issues are resolved, input of the TC 971 AC 522 CLSIDT. Refer to Exhibit 25.23.9-4 BMF ID Theft Indicators - TC 971 AC 522 CLSIDT - Closed and Confirmed as BMF ID Theft, for more information.

If	And	Then
<p>You have completed preliminary research and suspect the taxpayer is a victim of BMF identity theft and:</p> <ul style="list-style-type: none"> There is no identity theft indicator on TXMOD or BMFOLT, Or the indicators have been reversed 	<p>No other relevant controls in another function</p>	<ol style="list-style-type: none"> Input TC 971 AC 522 IDTCLM indicating an initial allegation of identity theft has been made by the taxpayer. Refer to Exhibit 25.23.9-2 BMF ID Theft Indicators - TC 971 AC 522 IDTCLM - Initial Allegation or Suspicion of BMF ID Theft You will suspend the case and request the taxpayer provide legible and complete documentation within 30 days and place the case in suspense for 45 days. If you do not receive a taxpayer response within 45 days from the date of request, close identity theft issue and resolve/address remaining issues as appropriate. Input TC 972 AC 522 NORPLY <p>Note: Provide an additional 15 days for responses from entities with foreign addresses.</p>

If	And	Then
There is already a TC 971 AC 522 IDTCLM identity theft indicator on TXMOD or BMFOLT	There is an IDRS control in another function with an earlier IRS received date	<ol style="list-style-type: none"> 1. Refer the taxpayer documents to the function with the open control via the ID theft referral process. 2. The employee in the function with the open control will suspend the case and request the taxpayer provide legible and complete documentation within 30 days and place the case in suspend for 45 days. 3. If the receiving function does not secure a taxpayer response within 45 days, close identity theft issue and resolve/address remaining issues as appropriate. Input TC 972 AC 522 NORPLY <p>Note: Provide an additional 15 days for responses from entities with foreign addresses.</p>

- (4) Once documents have been verified as complete and legible, you will mark the account with a TC 971 AC 522 IDTDOC and the Tax Administration Code designated for your BOD/Program. Refer to IRM 25.23.9.6.2, Taxpayer Supporting Documentation - TC 971 AC 522 IDTDOC, for more information.

Note: Refer to Exhibit 25.23.9-3 BMF ID Theft Indicators - TC 971 AC 522 IDTDOC - BMF ID Theft Documents Accepted, for more information.

25.23.9.8
(11-06-2020)
**Business Master File
(BMF) Identity Theft
Referrals**

- (1) BMF Identity Theft cases can be in any IRS function. Due to the complex nature of these cases, it is highly likely that a single case will cross functional lines and require the technical skill and systems access of another function or the case needs to be transferred to another function's ID theft treatment stream to be worked. In these situations, a referral to that function will be required. When a referral is sent for case assistance the function working the ID theft case will keep control of the case throughout the referral process.
- (2) IPSO developed Form 14566, BMF Identity Theft Referral to help employees in capturing required data when a referral to another function is needed. Use of the form will facilitate case processing.
- (3) When sending the referral, you must include a detailed explanation as to what factors contributed to the ID Theft determination. Include all relevant research information and clearly state facts of the case.

- (4) If contact is received by phone, once the research is completed, and ID theft is probable, refer the case to the proper function, annotate the referral with "phone contact" to make receiving function aware there will be no open control on the case.
- (5) If the case is being transferred to another function's inventory, the case control will remain open until the acceptance into the other function is confirmed.
- (6) When a referral is required for case assistance, the originating function will complete the Form 14566, BMF Identity Theft Referral, and send with supporting documentation to the designated BMF Identity Theft Liaison for processing via secure E-mail providing a **30-day** completion time frame. Refer to Exhibit 25.23.9-6 BMF Identity Theft Referral Form. Document on AMS/CII if a referral was sent, along with the details of the request. If working a case on CII, attach the referral to the CII case when sent and acceptance or guidance is received.
- (7) The BMF Identity Theft Liaison will acknowledge receipt of the referral within **three** business days.
- (8) If an assistance referral is sent, the receiving function's employee will take requested actions and return the BMF Identity Theft Referral via secure E-mail to the originator's liaison within **30** days of receipt.

Note: If the originating and receiving functions disagree over the requested action or the time frame for completion, the BMF ID Theft Liaisons work together to determine the correct procedures to follow. If the Liaisons are unable to work through their differences, the liaison will elevate through their management chain for resolution.

- (9) Once all requested actions have been taken, the functional employee will return the BMF Identity Theft Referral to their liaison, via secure E-mail. The liaison will then send it through the originator's BMF ID Theft liaison and they will return it to the employee. The functional employee providing assistance will document all the actions taken on the BMF Identity Theft Referral Form and AMS/CII if available.
- (10) If the contact with the taxpayer is on the phone, the CSR will research the account thoroughly to determine if there is a high probability of ID theft. If the CSR feels the account needs to be placed in the ID theft treatment stream of another function, complete the Form 14566, BMF Identity Theft Referral Form, and forward to the proper BMF ID theft liaison. For phone situations where the case is not already in an active inventory, the control base **will not** be opened by the phone CSR but by the function who retains the case in their inventory. The phone assistor will update AMS to reflect the research completed, the sending of the referral and to which function it was sent. If the case does not meet the criteria of the referral function, that function's liaison will return to the sending function's liaison. If the case will remain in their function, follow normal functional procedures for placing the case in the function's ID theft treatment stream.

25.23.9.8.1
(10-01-2025)
**Fabricated or Inactive
Employer Identification
Number (EIN)
Procedures**

- (1) A fabricated EIN is an EIN that was established for the sole purpose of defrauding the government through the filing of IMF and BMF false refund returns or income documents. An Inactive EIN belongs to a legitimate business whose business operations have ceased.

25.23 Identity Protection and Victim Assistance

- (2) You will need to 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 help you in determining the validity of the EIN.

#

- (3) Research IRPTRI to determine if the BMF entity filed Forms W-2. It will be necessary to research the IMF accounts if Forms W-2 were filed to determine if:

#

This information is necessary to determine if a referral is needed to be made for further research of the IMF filings and actions taken on the IMF accounts.

Note: Document this information on the referral.

- (4) All account actions must be taken prior to requesting the account be locked. See IRM 25.23.9.9.3, Posted Return on Either a Fabricated EIN or Inactive Account, for the required account action needed.
- (5) Take the following actions once the EIN is determined to be a fabricated or an inactive business.
- Update the BMF sort line to include "Identity Theft". This is to advise Submission Processing that this EIN has been considered "fabricated" and it should not be re-opened if a return is received. Inactive accounts may need to be unlocked later if determined to have valid return filings or taxpayer provided information that the business is active and legitimate.
 - Use Form 14566, BMF Identity Theft Referral to complete **one** referral to IP, RICS and CI. The referral to IP is to have the account locked with a TC 971 AC 524 and applicable MISC field reference. The referral to RICS is to add the EIN to their database of bogus and fabricated EINs as they relate to IMF/BMF filings. The referral to CI is to notify them that you have made a BMF identity theft determination.
- (6) Referral should include all research performed and document the reason it was determined the EIN is for a fabricated or inactive business.

#

- (8) Once the TC 971 AC 524 is input, the referral will be returned to the originator stating the input has been completed.

Reminder: Incomplete referrals will be returned to the originating liaison.

25.23.9.8.2
(10-01-2024)
**Referrals to Return
Integrity and
Compliance Services
(RICS)**

- (1) The RICS organization keeps a database of bogus and fabricated EINs as they relate to IMF/BMF filings. After exhausting all BMF and IMF research and a determination cannot be made as to the authentication of the EIN, it may be necessary to request assistance from RICS to have them check the EIN and related SSNs against their database. The Form 14566, BMF Identity Theft Referral will be used for this purpose.
- (2) Referrals to RICS for this purpose will be limited to situations where more information is needed to confirm the existence of BMF ID Theft.
- (3) After documenting all your findings and research on the Form 14566, BMF Identity Theft Referral, forward the referral to your BMF ID Theft Liaison. The liaison will review the form and if the form is complete, the liaison will send it to RICS using secure E-mail to: *TS EF Referrals. In the "Actions requested (required)" section of the form, check the "other" box and request RICS provide information confirming if this EIN was used to file fraudulent returns or if they have already flagged this EIN as fabricated or bogus.
- (4) The Entity Fabrication (EF) Team will review your referral and respond within 30 days by returning the Form 14566, BMF Identity Theft Referral, via secure E-mail. The EF team will respond that the account has been added to their scheme list or rejected as not involving BMF ID theft.
- (5) If there are questionable IMF returns filed with what has been determined to be a fabricated EIN, complete the referral form with all information pertaining to the EIN to RICS. They will initiate research into the IMF accounts. Document the sending of the referral on AMS/CII if a referral was sent, along with the details of the request. The control base will remain open while awaiting RICS response.
- (6) RICS may lock an EIN suspected of being fabricated and issue the taxpayer Letter 5263C, Entity Fabrication, requesting more information to verify the entity. Identify these accounts by the following:
 - An open control assigned on ENMOD to 1481400000 with a category code of TPPI and activity history showing POTENTEF
 - A posted TC 971 AC 524 on ENMOD containing BMF RICS EINFB2 in the MISC field.
- (8) If the taxpayer calls after issuance of Letter 5263C, Entity Fabrication, and the account contains the indicators listed above, follow the If/Then chart below.

#

#

If the taxpayer calls and	Then
The taxpayer claims they have no knowledge of the business referenced on the letter, questions the letter, or is asking for assistance relating to the letter.	Advise the taxpayer they must reply to the Letter 5263C and provide the requested information via fax or to the address on the letter. Caution: Do not provide (verbally or in writing) any information to the taxpayer that will provide them with the answers to any of the questions found on Letter 5263C. Advise the taxpayer they must provide the requested information to the IRS by replying to the 5263C letter via Fax or to the address provided on the letter.
Taxpayer says they did not receive a Letter 5263C, Entity Fabrication.	

#

25.23.9.8.3
(09-15-2020)
Referrals to Criminal
Investigation (CI)

- (1) CI keeps a database of IMF/BMF accounts under investigation. You may request CI check the EIN and related SSNs against their database after you’ve exhausted all BMF and IMF research options and still cannot authenticate the EIN. Use the Form 14566 , BMF Identity Theft Referral, for this purpose.

#

- (2) After documenting all your findings and research on the Form 14566, BMF Identity Theft Referral, forward the referral to your BMF ID Theft Liaison. The liaison will review the form and if the form is complete, the liaison will send it to the CI liaison. Document the sending of the referral on AMS or CII if a referral was sent, along with the details of the request.

Note: In the “Actions requested (required)” section of the Form, check the “other” box and document the type of referral: A search request of CI’s scheme database or notification of a BMF ID Theft determination.

- (3) CI will review your referral to determine if there is an open investigation related to the EIN and respond within 30 days by returning the referral form via secure E-mail with the appropriate response.

Reminder: Incomplete referrals will be returned to the originating BMF ID Theft Liaison.

- (4) The control on the case will remain open while awaiting CI’s response.

25.23.9.8.4
(10-01-2025)
Referrals to Lock the Account

- (1) After determining an EIN is fabricated or inactive, refer the case to your BMF ID theft Liaison using the Form 14566, BMF Identity Theft Referral, to request a TC 971 AC 524 be applied to the EIN. Be sure to document all your findings and research on the Form 14566.
- (2) The input of the TC 971 AC 524 will cause the posting of a TC 020 locking the account. The TC 020 will post one cycle after the TC 971 AC 524. The TC 020 is only visible using CC BMFOLE. A TC 020 with a prior 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.

Exception: The input of a TC 971 AC 524 with miscellaneous code ENTLOK will not post a TC 020. A TC 971 AC 524 with miscellaneous code ENTLOK only locks the entity information from being changed.

#

- (4) Prior to sending the referral to have a fabricated or inactive EIN locked, ensure:
- There are no balances remaining on the account.
 - There are no credits on the module.
 - A TC 971 AC 504 SPCL2 is input on the SSN of the cross reference for the EIN. Refer to IRM 25.23.4.2(6) for more details.
 - The sort name line is changed to “Identity Theft”. If there is currently a name on the sort name line, move it down to the in care of name line. Then input “Identity Theft” on the sort name line.

- e. Document the sending of the referral on AMS along with details of the request. If working a CII case, attach the referral and a PDF print of the original entity (CC ENMOD) to the case. If CC ENMOD is unavailable then CC BMFOLE can be used in its place. The referral and the PDF print of the original entity should be included in the request to have the account locked.

Note: For account lock reversal requests 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) Once the TC 971 AC 524 is input, IP will return the referral to the originator stating the input was completed.
- (6) Do not close the case until the TC 971 AC 524 and TC 020 are posted on the account and all other account actions have been taken.

25.23.9.8.5
(09-15-2020)

**Referrals to Combined
Annual Wage Reporting
(CAWR)**

- (1) In situations where identity thieves filed false income documents, contact the CAWR function to alert them to the false income documents.
- (2) Document all your findings and research on the Form 14566, BMF Identity Theft Referral and forward it to your BMF ID Theft Liaison. Include all pertinent documentation and document the referral on AMS or CII if the referral was sent. Your BMF Liaison will forward the referral to the CAWR Liaison using secure E-mail.

Reminder: If you are requesting an adjustment action, include all required forms and documentation with your request.

- (3) CAWR will acknowledge receipt of your referral within 30 days by returning the Form 14566 , BMF Identity Theft Referral , via secure E-mail.

25.23.9.9
(10-01-2025)

Account Actions

- (1) Once it is determined there is ID theft, it is necessary to take the proper account actions to balance the account. If the posted return is determined to be an ID theft return, **DO NOT** leave the return on the account. The account must be corrected. If the invalid return is the only one posted, it must be backed out. If the EIN owner also filed a return, follow the procedures in IRM 25.23.9.9.1, Duplicate/Amended Return Research.
- (2) It will be necessary to determine if a refund has been lost, or if there are offsets in the module, or identify other account issues affected by the filing of the ID theft return.
- (3) All issues relating to ID theft **MUST** be completed before the ID theft case is closed. This includes any related balance due issues such as an installment agreement that may have been affected by a refund offset. If an installment agreement was full paid by an offset, reinstate the agreement once the offset is reversed. If there have been levies or liens filed relating only to the ID theft return, they must be removed following normal procedures. Collection Advisory contacts can be found under the Who/Where tab on the SERP Home Page on the *Advisory Units Contact List*.

- (4) Research the account to ensure the address is correct. Update the address if appropriate. If the original return is an ID theft return, the address may have been changed when the return was processed.
- (5) If the “invalid” return posted first, back out the first return (do not net; exceptions can be made for imminent statute issues). This will provide a clearer notice to the taxpayer reflecting the adjustment figures they had on the “valid” return.
- (6) Employees working the various inventories are usually the first to identify trends and schemes. If you see returns that all seem to be fitting into a pattern of questionable filings and are potential ID theft issues, forward the information to your functional BMF ID Theft Liaison for evaluation to headquarters. See *Identity Theft BMF Home (irs.gov)* for liaison contacts located on the BMF ID Theft website.

25.23.9.9.1
(09-15-2020)
**Duplicate /Amended
Return Research**

- (1) As ID theft incidents increase, ID thieves are constantly changing ways of obtaining fraudulent refunds from the IRS. Those employees that work paper cases and answer phones are often the first to recognize a scheme or an invalid return. When working any inventory, ID theft should always be in the back of your mind. When working duplicate or amended returns, it is necessary to ensure that all the returns have been filed by the true EIN owner or authorized third party.
- (2) ID theft returns need to be handled differently. Returns that have been considered ID theft will be nullified and the ‘valid’ return input on separate adjustments.
- (3) Prior to making any adjustments on the account, thorough research must be completed. The determination that all returns have been filed by the EIN owner or authorized third party needs to be made. There are some quick checks that should be completed to help in determining if the return in question is potentially an ID theft return and more research will be needed. When working duplicate or amended returns ask yourself (this list is not all inclusive):

#

If you review the return and feel the information does not follow normal BMF filings or if any of the conditions listed above exist, more research will be needed prior to inputting any adjustments.

#

#

- #####

- 25.23.9.9.2
(10-01-2024)
**Invalid Return Posted
First and Valid Return
(Refund or Zero
Balance)**

- (1) Once it is determined that the original posted return is an ID theft return, that return is considered a nullity. This means the information on the account relating to the posted original return is not valid. This includes the Assessment Statute Expiration Date (ASED) posted on the account.
- (2) Determine if the ASED needs to be addressed 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 than the date posted on the original return on the module. The ASED will be updated to the receive date plus 3 years.

25.23.9.9.2

taxpayer had filed an extension on 4-10-2020. The valid return was received on 8-14-2020, the ASED for the valid return would need to be updated to 8-15-2023.

Note: All business units should review the ASED to prevent a barred assessment

- (3) Input the new 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 more information.
- (4) If the original return is the ID theft return, research the account to determine if the address has been changed by the posting of the return. If the address has been updated, change the address back to the correct business address.
- (5) Research the account to determine if any overpayment has offset to any other module (IMF and BMF). Reverse all offsets using the proper transaction codes.

Caution: Input a TC 570 as a secondary transaction code on the credit side of the credit transfer to prevent the release of any overpayment in the module.

- (6) Determine if the refund has been lost. If there is a TC 846/840 on the module and the refund cannot be stopped, the account must be balanced and the lost refund credited back to the account. This is done by moving credit from the 1545 account back into the module. Refer to IRM 25.23.9.9.6, Lost Refund. Input a secondary TC 570 to hold the credit when the TC 841 posts. Do not adjust the account until the TC 841 has posted.
- (7) For Form 1120, if the refund was not issued and there was a request for direct deposit, input a TC 971 AC 850 to stop any overpayment from direct depositing to the ID thief's account.
- (8) Back out the ID theft return. Back out all transactions and item/credit references associated with the return. Input the adjustment with a HC 4. When backing out the return ensure that all associated penalties, interest and fees that were manually assessed have been included in the adjustment.
- (9) Input the second adjustment to reflect the taxpayer's valid return. Post delay this adjustment 1 cycle to ensure all prior account actions have posted.
- (10) If there is a TC 130 on the XREF SSN which relates only to the ID theft issue, reverse the TC 130 using CC REQ77. Research the account thoroughly to ensure that all liabilities on the account are related to the ID theft issues only.

Example: Taxpayer says he closed the business in 2012 and the BMF ID theft issue is for 2016. Research shows the taxpayer has an outstanding liability for 2012 and 2016. While the liability for 2016 will be removed for ID theft, the 2012 liability is still valid for 2012 and the TC 130 should not be reversed in this case.

25.23.9.9.3
(05-09-2022)
**Posted Return on Either
a Fabricated Employer
Identification Number
(EIN) or Inactive
Account**

- (1) If there is a return posted to the account and it has been determined the EIN is fabricated or inactive, the account needs locked down. This means that **all** posted transactions on the module will need to be reversed.
- (2) Back out all posted returns from the involved modules. Use HC 4 on the adjustment to prevent any credits for refunding. For inactive accounts, only back out the returns/transactions created from the identity theft.

- (3) If there are any manually assessed penalties, interest or fees associated with the assessments on the module, reverse them. Once all adjustments post the balance on the account should be “zero”.
- (4) 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 the payments should be applied, move the payment to excess following normal procedures.
- (5) If there are offsets or payments belonging to the ID Theft victim, determine if the payments are eligible for refund. If the statute has expired on the payments move them into excess following normal procedures.
- (6) If there has been collection action taken, such as a lien filing or levy situations, they must be released.
- (7) If there is a TC 130 on the XREF SSN which relates only to the ID theft issue, reverse the TC 130.
- (8) Under the X-REF SSN, input TC 971 AC 504 MISC SPCL2 with EIN as XREF TIN.
- (9) If it is determined to be a fabricated or inactive EIN, see IRM 25.23.9.8.1, Fabricated or Inactive EIN Procedures, for more action requirements.

25.23.9.9.4
(09-15-2020)
**Invalid Return Posted
First and the Valid
Return is a Balance Due**

- (1) If the “invalid” return posted first and the valid taxpayer filed a balance due return with the balance still unpaid or was paid after the original return due date, it is necessary to properly handle the account so the FTP penalty can be systemically computed on the valid taxpayer’s return.

#

- (4) It is imperative the account be properly handled to ensure the correct amount of FTP penalty is charged.
 - a. It is necessary to completely back out the invalid return, DO NOT net with the valid return. Back out any associated penalties other than a bad check penalty and the FTP penalty. The FTP penalty will automatically reverse when the account is backed out.

Note: Address the bad check penalty as a separate issue. Determine if the payment was made by the alleged ID thief or by the business. If payment **was not** made by the business follow IRM 20.1.2.2.6.3, Wrong Return Posted First, for procedures to abate the penalty.

- b. Take all other account actions needed to balance the account. This would include any offset reversals, moving of refunds or crediting lost refunds back into the account. Include all proper hold codes where applicable.
- c. Compute the “tax shown” on the “valid” return. This is the amount of tax the taxpayer figured they owe, minus any taxpayer computed refundable and prepaid credits. Follow the instructions in IRM 20.1.2.2.6.3, Wrong Return Posted First, for computing “tax shown.” This amount will be entered in the adjustment using Item Reference Number (IRN) 871. The input of the IRN 871 tells the computer the tax the taxpayer expected to owe on their return and the amount of tax that will be assessed FTP penalty from the due date of the return. The computer will recognize ES payments, FTD penalty and refund reversals (TC 841) in the calculation of the FTP penalty.
- d. Determine if the ASED needs to be addressed prior to inputting any adjustment. If there is a duplicate return posted 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 than the date posted on the original return on the module. The ASED will be updated to the received date plus 3 years.

Example: The return due date is 4-15-2016 and the ID theft return posted 4-14-2016. The ASED for this return would be 4-15-2019. The valid taxpayer had filed an extension on 4-10-2016. The valid return was received on 8-14-2016, the ASED for the valid return would need to be updated to 8-14-2019.

- e. Input the new ASED with a TC 560 using TC REQ77 as appropriate. See IRM 25.6.1.6.14 Criteria for Establishing a Statute of Limitations.
- f. Math verify the return and complete the normal computations for determining tax, credits and other penalty amounts to be entered on the adjustment.
- g. Input the adjustment using all applicable item reference and credit reference numbers with a Priority Code 2, Hold code 0 (zero) and the proper IRN 871 amount. The PC 2 allows the computer to recognize the need to compute the FTP penalty back to the RDD for the lesser of the IRN 871 amount or the “tax assessed” on the return. For example, if there is a discrepancy between what the taxpayer thinks they owe and what is calculated, such as a math error, the FTP penalty will be correctly computed. The HC 0 allows the notice to generate with the correct FTP penalty calculation. The computer will recognize any payments, credit elect, withholding and refundable payment credits applied against the tax owed and adjust the FTP penalty computation accordingly.

Caution: Any tax or refundable tax credits posted prior to the priority code “2” adjustment are ignored in the FTP penalty computation. This is the reason the original return needs to be completely backed out.

- h. Input the proper post delay(s) on the adjustment to allow all account transactions to post prior to the adjustment.
- i. See IRM 20.1.2.2.6.3, Wrong Return Posted First, for more information.

Example: Invalid return was filed 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) with PC 2. The

25.23 Identity Protection and Victim Assistance

computer will compute the FTP from the RRD on the \$1,000 (the lesser of the tax assessed or the IRN amount). Since the taxpayer was unaware of the \$500 tax increase, he has the 21 days from the 23C date to pay the \$500 without FTP being charged.

Example: The valid taxpayer had made several ES payments totaling \$5,000. An invalid return posts requesting a refund of \$4,000. Due to the ES payments made, a refund of \$9,000 is issued to the invalid taxpayer. The invalid return is backed out and a credit of \$9,000 is moved into the module from the 1545 account, posting a TC 841 for \$9,000. After all account actions are complete the account is going to now show the correct credit of \$5,000. The valid return is showing a balance of \$2,000 after applying the ES payments made. The tax shown on the valid return is \$7,000 with no refundable tax credits. Since there is no discrepancy between the taxpayer's figures and the math verified figures on the valid return the TC 290 and IRN 871 figures will be the same. The adjustment to post the valid return is: TC 290 \$7,000 with the IRN 871 \$7,000 with PC 2 and HC 0. The computer will recognize the TC 841 as cancelling the refund and will read the payments and recognize the balance owed as \$2,000. In this situation, the taxpayer is going to get charged FTP from the RDD until the balance of the \$2,000 is paid in full.

25.23.9.9.5 (11-06-2020) Statute Implications

- (1) If the assessment of the taxpayer's true return will include a tax increase and after determining the ASER for the taxpayer's valid return is within 90 days, then statute procedures must be followed. Follow procedures in the IRM 25.6.1.5, Basic Guide for Processing Cases with Statute of Limitation Issues.
- (2) In situations where the taxpayer is claiming ID theft on an older year and there is a balance due, there may be payments on these accounts from offsets, levy payments, or payments made by the taxpayer to avoid collection activities. Depending on the circumstances of the case and if the payments are creating an overpayment, it is necessary to determine if the payments are refundable. Determine if the payments or offsets meet the RSED rules prior to allowing any refund from generating. See IRM 25.6.1.7.2, Time when Payments and Credits are Considered to be Made.

25.23.9.9.6 (09-15-2020) Lost Refund

- (1) If an ID theft return (original or amended) has been processed and a refund was issued to the Identity thief, credit back the ID theft refund amount into the taxpayers account to balance the account. This is done by moving the credit from the ID Theft 1545 account.
- (2) Prep and post the TC 841/700 prior to backing out the invalid return.
- (3) Move all offsets prior to moving the credit from the 1545 account.
- (4) 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. The 1545 account is the debit account and the taxpayer's account is the credit account.
- (5) If part of the refund was offset and the credit is being returned to the module, only the part of the refund that is unrecoverable will be moved from the 1545 account.

- (6) To input the reversal using command codes IDT48 or IDT58:
 - a. See IRM 2.4.61-1, IDT48, RPM48 or CSO48 Input Format
 - b. See IRM 2.4.61-2 ,IDT58, RPM58 or CSO58 Input Format
- (7) Suspend case and monitor for the posting of the TC 841/700.

25.23.9.9.7
(10-01-2021)
**Request for a New
Employer Identification
Number (EIN) by a
Taxpayer Who Is a
Victim of Identity Theft**

#

- (2) For the IRS to consider the issuance of a new EIN based on identity theft, the ID theft **must have** federal tax administration impact. These would include:
 - a. Fraudulent returns filed under this EIN. This would include original or amended returns
 - b. Filing of fraudulent income documents. This would include Forms W-2, Form 1099 series, etc.
- (3) If research shows there has been tax impact on the account and the taxpayer insists on a new EIN, advise them to:
 - a. Complete a new Form SS-4, Application for Employer Identification Number.
 - b. Complete Form 14039-B, Business Identity Theft Affidavit.
 - c. Attach the Form 14039-B to the Form SS-4 and mail to:
Ogden BMF Entity
1973 N Rulon White Blvd.
Mail Stop 6273
Ogden, UT 84404
- (4) When the forms are received in Entity, a new EIN will be assigned and then merged with the old number. The taxpayer will receive notification when the new EIN is assigned.
- (5) Take all the required account actions that need to be completed to make the account whole.
- (6) In situations where the taxpayer says their EIN was stolen and used in ways other than the federal filing of returns or income documents, the IRS will not issue a new EIN to the existing business on that basis.
- (7) If the taxpayer insists on a new EIN even though there is **no tax impact**, they may shut down the current business to obtain a new EIN. They may:
 - a. File final returns for all open filing requirements. This will close out the current business.
 - b. Contact the state for approval of the new business name.
 - c. Submit a new Form SS-4, Application for Employer Identification Number, with a new business name or apply on-line. If submitting the Form SS-4, Application for Employer Identification Number, advise the taxpayer to check the "Other" box under line 10 and specify the reason for the new EIN. They will also need to supply the old EIN on line 18. This will help to prevent the research from showing a duplicate EIN if the new name is like the old.

- d. Advise the taxpayer to send the completed Form SS-4 to:
Internal Revenue Service
Attn: EIN Operation
Cincinnati, OH 45999
Fax: (855) 641-6935
- e. They will receive notification CP 575 when the new EIN is assigned.

25.23.9.10
(09-15-2020)

Providing Copies of Tax Returns or Income Documents Where ID Theft is Suspected or Proven

- (1) The taxpayer may request copies of tax return and/or information documents associated with potential or confirmed ID theft issues. The IRS will honor these requests under specific circumstances. The information on these returns is considered to contain information that belongs to both the true taxpayer as well as the ID thief. Only the information that applies to the true taxpayer can be disclosed. This consists of only the information that can be used to determine tax liability. Requests can be for copies of:

- a. Tax Returns
- b. Income Documents

Reminder: In both situations, it is important to remember that only the information that can be used to determine the victim-taxpayer's liability can be disclosed in situations where ID theft is suspected or confirmed. Information such as other TINs, banking information, and addresses cannot be disclosed. See IRM 25.23.9.10.2, Redacting Information, for more information.

- (2) Prior to releasing any information, it is necessary to determine:
 - a. If the taxpayer's ID theft is related to a legitimate business (active or inactive).
 - OR
 - b. If the taxpayer's issue is related to a fabricated EIN situation where the taxpayer claims their personal information was stolen and used to obtain the EIN.

(3) If it is a legitimate business (active or inactive):

- a. The taxpayer may be disclosed information about any questionable filings to help in the determination as to whether the filings are in fact fraudulent. This goes for both tax return and income documents information.
- b. The return and/or income document information remains with the business even if it is later determined that the return or income information is fraudulent. If the determination has already been made, the taxpayer is still entitled to the information because at the time of filing all the information represented a possible liability for the business.
- c. See IRM 25.23.9.10.2, Redacting Information, to determine what information must be redacted.

(4) If the business is fabricated:

- a. If the taxpayer says they have no association with the business and it is determined that the taxpayer's personal information was stolen to establish the EIN, no return or income documents information can be disclosed to the taxpayer. This is because the taxpayer does not have individual liability for the business and the information contained within any of the documents is not considered as belonging to the taxpayer.

Under **no** circumstances should any information be shared if the taxpayer is claiming no association to the business.

25.23.9.10.1
(09-15-2020)
**Sending Redacted
Information**

- (1) If a taxpayer suspects BMF ID theft, they may contact us by phone or in writing. In either case all responses to these requests will be mailed **ONLY** to the address of the business. If the return in question changed the taxpayer's "good" address, complete research to determine the current address of the business. Utilize outside resources if necessary, such as Google or Google Maps to verify the address.
- (2) **Phone Contact-** If the taxpayer contacts us by phone and after complete research there is potential ID theft, the taxpayer may want copies of the return or forms in question to verify the non-filing of the information. Document on AMS with the caller's name, and what documents were sent.
- (3) **Paper case-** If the request is received by paper, ensure the taxpayer has provided all the needed information to complete the request. This would include the EIN, forms in question and Tax periods.
- (4) In either request type, it is not necessary to redact and send all requested items if the number of documents is too large. For example, the number of Forms W-2 filed may exceed 1,000 forms. Redact and send only enough of the information for the taxpayer to make the determination that they did not file the information. In this situation, advise the taxpayer they will be receiving only a part of the information because the volume is too large to redact.

25.23.9.10.2
(11-30-2023)
Redacting Information

- (1) If the taxpayer is requesting copies of potential ID theft returns or income documents, obtain the documents using the information available on TDS, IDRS or MeF for electronically filed returns. For employees utilizing the BTR tool, information from the screens can be printed by going to either the print icon or "file" for the print option. Once the information is accessed:
 1. Print the information as a PDF file; use the CII number as the case name and save to your SBU folder. (Hint: Check your SBU folder prior to closing the file to ensure the file is saved).
 2. Once the PDF file opens, click on the **"Tools"** menu.
 3. Under **"Protect & Standardize"** click on **"Redact"**.
 4. Using the mouse pointer, click and then drag over the information to be masked.
 5. Continue to mask all required information.
 6. Select **"Apply"** under the protection menu when all masking is complete. Another dialogue box will appear, click **"Continue"**. The boxed areas will then turn black for the redaction.
 7. Save file in SBU folder - include CII case ID in the file name. The page can now be printed normally and sent to the taxpayer.
- (2) **What needs to be redacted-** While the information that pertains to the determination of the victim-taxpayer's tax liability can be disclosed, information not relating to the computation of liability cannot be disclosed. It is necessary to determine which information must be redacted prior to sending the taxpayer the requested documents. Information that needs to be redacted is (these lists are not all inclusive):
 - a. **Tax Forms**
 - TINs- Mask entire number except the last four digits. This includes all

25.23 Identity Protection and Victim Assistance

identifying identification numbers listed on the return or attached schedules if different from the EIN owner's.

- Business or Corporation names- Mask entire business name except the first four letters of the first name and the first four letters of any subsequent name on the name line. This includes all names listed on the return or attached schedules if different from the EIN owner's.
- Addresses- Mask the entire address except the first six numbers or letters of the street address line including spaces. This includes all addresses listed on the return or attached schedules if different from the EIN owner's.
- Preparer Identification Number- Mask entire number except the last four digits of DPIN or PTIN.
- Telephone number if not the number recorded on the account- Mask entire number except for last four digits.
- Banking information- this includes the routing and account numbers if present- Mask entire number except for last four digits.
- IP address if present- Mask entire IP Address except the last four digits of IP address.
- Software information if present- Mask entire Software ID except the last four digits of Software ID.
- All signatures on the tax return, forms, or schedules- Mask entire signature.

b. **Income Document**

- Employer/Payer address if different from the EIN owner's- Mask the entire address except the first six numbers or letters of the street address line including spaces.
- Employer/Payer name if different from the EIN owner's- Mask entire name except the first four letters of the recipients last name or business name.
- Taxpayer/Recipient/Filer name- Mask entire name except the first four letters of the recipient's last name or business name.
- Taxpayer/Recipient/Filer address if different from the EIN owner's- Mask the entire address except the first six numbers or letters of the street address line including spaces.
- Taxpayer/Recipient/Filer TIN (Identification number)- Mask entire number except the last four digits.
- Employer/Filer State ID number if different from the business's federal number
- Account number
- PSE's name and telephone number- Forms 1099-K, Payment Card and Third-Party Network Transactions

For examples on redacting BMF/IMF transcripts please see IRM 25.23.3.2.6.4, Manual Masking of MeF and TRDBV Fraudulent Return Request Transcript

- (3) If the case is being worked through CII, attach a copy of the redacted print to the CII case.

25.23.9.10.3 (10-01-2025) **BMF Transcripts and Identity Theft**

- (1) As outlined in IRM 21.2.3.5.9, Transcripts and Identity Theft for Businesses, Transcript Delivery Service (TDS), is programmed to restrict the delivery of transcripts to external users when certain identity theft indicators are present for the tax year requested. These external users include tax professionals accessing TDS via e-Services and business taxpayers using Business Tax Accounts (BTA) online.

##

- (3) When receiving inquiries involving transcript requests with identity theft use IRM 25.23.11.6.5.2, BMF Transcripts and Identity Theft.

This Page Intentionally Left Blank

Exhibit 25.23.9-1 (01-14-2025)

Transaction Code (TC) 971 Action Code (AC) 5XX- MISC Codes

1. BOD

Business Operating Division	Definition
AP	Appeals
CI	Criminal Investigation
LB	Large Business and International
SB	Small Business & Self Employed
TA	Taxpayer Advocate Service
TE	Tax Exempt Government Entities
WI	Wage and Investment

2. Program Name

Note: If your specific function is not listed below, elevate to your BOD/Function identity theft liaison. The liaison will contact IPSO and request an alternative until programming can be implemented for more codes.

Caution: Field Assistance employees are **not** profiled to input identity theft indicators on BMF accounts. Field Assistance employees will refer the case to the proper functional liaison for research and the marking of the accounts in question.

Function	Definition
AP	Appeals
RC	Refund Crimes
LBI	Large Business and International
IPSO	Identity Protection Strategy & Oversight
ACS	Automated Collection System
AM	Accounts Management
ATTI	Abusive Transactions Technical
AUR	Automated Underreporter
CA	Case Advocate
CAWR	Combined Annual Wage Reporting
CE	Correspondence Exam
CSCO	Compliance Services Collection Operations
EXCISE	Excise Tax
FC	Field Collection
FE	Field Exam

Exhibit 25.23.9-1 (Cont. 1) (01-14-2025)

Transaction Code (TC) 971 Action Code (AC) 5XX- MISC Codes

Function	Definition
FLDADV	Field Advisory
FRIV	Frivolous Filer
FUTA	Federal Unemployment Tax Act
FLDINSLV	Field Insolvency
RICS	Return Integrity & Compliance Services
SPCLTX	Employment Specialty Tax
TDI	Tax Delinquency Investigation
TEFRA	Tax Equity and Fiscal Responsibility Act of 1982
EF	Entity Fabrication
ACSS	Automated Collection System Support
TEGE	Tax Exempt & Government Entities

3. BMF Tax Administration Source Codes

Action Code	Term/Acronym	Definition
522	IDTCLM	Applied to the TXMOD of the applicable MFT and Tax Period when an initial claim or suspicion of BMF identity theft is supported by preliminary research
522	IDTDOC	Applied to the TXMOD of the applicable MFT and Tax Period when the taxpayer provides complete and legible Form 14039 or Form 14039-B, and supporting documents for a BMF identity theft issue.
522	CLSIDT	Applied to the TXMOD of the applicable MFT and Tax Period when all identity theft issues are resolved
524	EINFAB	Applied to entity when EIN is fabricated and the account is locked.
524	EINFB2	Applied to entity when EIN is suspected of being fabricated and the account is locked
524	INACT3	Applied to a legitimate entity when EIN has been inactive for 3 years and the account is locked
524	INACT5	Applied to a legitimate entity when EIN has been inactive for 5 years and the account is locked
524	BSCLSD	Applied to a legitimate entity when business has been closed and the account is locked.
524	DFUNCT	Applied to a legitimate entity when business is defunct (no longer in operation) and the account is locked.

Exhibit 25.23.9-1 (Cont. 2) (01-14-2025)**Transaction Code (TC) 971 Action Code (AC) 5XX- MISC Codes**

Action Code	Term/Acronym	Definition
524	FNLRTN	Applied to a legitimate entity when business has filed a final return and the account is locked.
524	NOFR	Applied to a legitimate entity when business has no filing requirements and the account is locked.
524	ENTLOK	Applied to a legitimate entity when identity theft is confirmed, and the entity is locked to prevent name, address, and responsible party updates.

Exhibit 25.23.9-2 (09-15-2020)**Business Master File (BMF) Identity (ID) Theft Indicators - Transaction Code (TC) 971 Action Code (AC) 522 IDTCLM - Initial Allegation or Suspicion of Business Master File (BMF) Identity (ID) Theft**

BMF identity theft indicators are placed on TXMOD for all MFTs and Tax Periods affected by identity theft. TC 971 AC 522 IDTCLM is applied to all accounts when identity theft is alleged or suspected by the taxpayer and research verifies the probability of ID theft. The taxpayer has not yet provided any supporting documents and the case is assigned and controlled.

Obtain the following information:

- EIN
- MFT and Tax Period of the identity theft incident
- Navigate to TXMOD for the selected MFT and Tax Period

Enter REQ77

FRM77 is displayed for the selected MFT and Tax Period

Enter the TC 971 AC 522

- TC> Enter the TC with 971
- TC971/151-CD> Enter 522
- TRANS-DT is auto populated with the current date
- Enter SECONDARY-DT-If taxpayer identified, enter the IRS receive date or the date of the call. If IRS determined, enter the date the IRS suspected identity theft after concluding preliminary research. The date cannot be the current date, it must be before the current date (you can use yesterday's date).
- Enter MISC> Enter your specific BOD/Program name, refer to Exhibit 25.23.9-1 TC 971 AC 5XX - MISC Codes.

Example: If you are a Combined Annual Wage Reporting employee you will enter the following when you identify a BMF identity theft situation:

SB CAWR IDTCLM

Example: If you are a BMF Adjustment employee you will enter the following when you identify a BMF identity theft situation:

WI AM IDTCLM

Note: If the account (MFT and Tax Period) already contains a TC 971 AC 522 IDTCLM do NOT input a second code.

Exhibit 25.23.9-3 (10-01-2022)

Business Master File (BMF) Identity (ID) Theft Indicators - TC 971 AC 522 IDTDOC - BMF ID Theft Documents Accepted

BMF identity theft indicators are placed on TXMOD for the MFT and Tax Period affected by identity theft. TC 971 AC 522 IDTDOC is applied to all accounts when the taxpayer has provided a complete and legible Form 14039 or Form 14039-B and supporting documents.

Obtain the following information:

- EIN
- MFT and Tax Period of the identity theft incident
- Navigate to TXMOD for the selected MFT and Tax Period

Enter REQ77

FRM77 is displayed for the selected MFT and Tax Period

Enter the TC 971 AC 522

- TC> Enter the TC with 971
- TC971/151-CD> Enter 522
- TRANS-DT is auto populated with the current date
- Enter SECONDARY-DT -Enter the IRS received date of the documents provided by the taxpayer in support of the identity theft allegation.
- Enter MISC> Enter your specific BOD/Program name, refer to Exhibit 25.23.9-1 **TC 971 AC 5XX-MISC Codes**

Example: If you are a Field Collection employee you will enter the following when you identify a BMF identity theft situation:
SB FC IDTDOC

Example: If you are a BMF Adjustment employee you will enter the following when you identify a BMF identity theft situation:
WI AM IDTDOC

Note: If the account (MFT and Tax Period) already contains a TC 971 AC 522 IDTDOC do NOT input a second code. An account may contain both a TC 971 AC 522 IDTCLM and a TC 971 AC 522 IDTDOC.

Exhibit 25.23.9-4 (09-04-2015)**Business Master File (BMF) Identity (ID) Theft Indicators - TC 971 AC 522 CLSIDT - Closed and Confirmed as BMF ID Theft**

BMF identity theft indicators are placed on TXMOD for the MFT and Tax Period affected by identity theft. TC 971 AC 522 CLSIDT is applied to all accounts when all actions to resolve the identity theft issues have been taken and posted and the taxpayer is notified.

Obtain the following information:

- EIN
- MFT and Tax Period of the identity theft incident
- Navigate to TXMOD for the selected MFT and Tax Period

Enter REQ77

FRM77 is displayed for the selected MFT and Tax Period

Enter the TC 971 AC 522

- TC> Enter the TC with 971
- TC971/151-CD> Enter 522
- TRANS-DT is auto populated with the current date
- Enter SECONDARY-DT -Enter the date the identity theft issues were completely resolved. The date cannot be the current date, it must be before the current date. (you can use yesterday's date).
- Enter MISC>Enter your specific BOD/Program name, refer to Exhibit 25.23.9-1 **TC 971 AC 5XX-MISC Codes**

Example: If you are a Field Collection employee you will enter the following when you identify a BMF identity theft situation:
SB FC CLSIDT

Example: If you are a BMF Adjustment employee you will enter the following when you identify a BMF identity theft situation:
WI AM CLSIDT

Note: If the account (MFT and Tax Period) already contains a TC 971 AC 522 CLSIDT do NOT input a second code.

Exhibit 25.23.9-5 (02-04-2020)
Reversing Business Master File (BMF) Identity (ID) Theft Indicators - Transaction Code (TC) 972 Action Code (AC) 522

If you subsequently determine an account is NOT affected by identity theft, you will need to reverse all the identity theft indicators applied to the account.

Obtain the following information:

- EIN
- MFT and Tax Period of the identity theft incident
- Navigate to TXMOD for the selected MFT and Tax Period

Enter REQ77

FRM77 is displayed for the selected MFT and Tax Period

Enter the TC 972 AC 522

- TC> Enter the TC 972.
- TC971/151-CD> Enter 522.
- TRANS-DT> Enter the transaction date of the TC 971 AC 522 being reversed.
- SECONDARY-DT> Enter the secondary date of the TC 971 AC 522 being reversed. Exception: RICS systemic reversals do not require a secondary date. If no secondary date is shown on the TC 971 AC 522 IDTCLM, RICS employees must input the transaction date of the TC 971 AC 522 being reversed in this field.
- MISC> Enter your BOD Program Code followed by the reason why the BMF Identity Theft Indicator is being reversed using the table below.

Reason for BMF ID Theft Reversal	Reversal Code
<p>If, after completing a case analysis, you have determined ID Theft did not occur.</p> <p>Example: Taxpayer contacts the IRS believing to be a victim of identity theft. After careful case analysis and review, the employee determines this is a mixed entity case, no identity theft occurred.</p>	NOIDT- Document on AMS/CII why ID theft is not indicated.
The taxpayer did not respond to your request for supporting documentation.	NORPLY
The BMF ID Theft indicator was applied due to a typographical mistake or another internal mistake.	IRSERR
The original identity theft incident claim was determined to be false/untrue.	FALSE
The reason for the 971 reversal does not meet any of the above reason descriptions	OTHER- Document AMS/CII the reason for the reversal.

Exhibit 25.23.9-6 (10-01-2024)**Business Master File (BMF) Identity Theft Referral Form**

The table below provides information for each field on the Form 14566 , *BMF Identity Theft Referral*

Note: All business units should follow the instructions below when completing the referral Form 14566.

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 periods.
Actions Requested	Check all actions being requested Note: There are two actions listed under “IMF Actions” all other actions are BMF.
Explanation for ID Theft Determination (Required Field)	Provide a detailed explanation to the receiving function of what was found that determined the case as IDT. Attach documents that prove your determination when available. If Form 14039 or Form 14039-B is present, attach the form to the secure e-mail when referring the case. Note: It is also helpful to show if the BTR tool was used for your research.
Employee Name and Function	Full name of person submitting the Form 14566 and the function they belong to.
Telephone Number	The initiator’s phone number in case contact is needed.
Date	The date the Form 14566 is prepared or sent.

Caution: Incomplete or inappropriate BMF Identity Theft Referrals may be returned to the originator for more case building, delaying case resolution.

The receiving function will be responsible for documenting the actions taken.

Exhibit 25.23.9-7 (01-03-2020)

Business Master File (BMF) Identity Theft Research Requirement

The table below was developed to help you with some of the research needed to help in making a BMF ID theft determination.

Action	What are you looking for?	Research Tools and Command Codes
Research the EIN for: <ul style="list-style-type: none"> • Date established • X-REF TIN (s) • Address • Filing requirements and history • Business Close Date • Business name - Primary and sort name • Entity Type • Third Parties 		BMF ID Theft Research tool (BITR) Document 6209 BMFOLE INOLES ENMOD FINDE CFINK RFINK DDBMF Note: DDBMF: shows Entity, Date Established, PTIN, X-REF, Limited Return (including 3 years of prior filings), BMF IDT and Frivolous Filter information.

Exhibit 25.23.9-7 (Cont. 1) (01-03-2020)
Business Master File (BMF) Identity Theft Research Requirement

Action	What are you looking for?	Research Tools and Command Codes
Entity Research		
Research all X-REF TINS	BMF: Research for possible successor or parent companies, possible mixed entities IMF:	BMF ID Theft Research tool (BITR) BMFOLE INOLES ENMOD IMFOLE FTBOL DDBMF

#

#

Exhibit 25.23.9-7 (Cont. 2) (01-03-2020)

Business Master File (BMF) Identity Theft Research Requirement

Action	What are you looking for?	Research Tools and Command Codes
Account Research	BMF: <ul style="list-style-type: none"> Research for open controls or ID theft case already being worked Check for ID theft indicators on prior years or MFTs Research for prior account assessments. CAWR, SFR/6020b, or Exam may open or closed issues. Some of these issues may be the result of default assessments/ no replies, which may show a possible fabricated EIN. Additional research or contact with the taxpayer may be necessary IMF: Check the x-ref SSN accounts to see if there are any ID theft or IVO indicators for the tax year in question on the entity. This may show ID theft.	TXMOD BMFOL/IMFOL AMS/CII History and Notes Document 6209
Payment Research		TXMOD BMFOLT RTR EFTPS BMFOLP

#

Business Master File (BMF) Identity Theft Research Requirement

Action	What are you looking for?	Research Tools and Command Codes
IRPTR Research		IRPTR BMFOLU PMFOL BMF ID Theft Research tool (BITR)
Refund Research		TXMOD BMFOLT IMFOLT DDPOL

