IRM PROCEDURAL UPDATE

DATE: 10/16/2023

NUMBER: wi-25-1023-1020

SUBJECT: IDTVA Timeframes; New Digital Form 14039 on irs.gov; ID.ME Call Replies

AFFECTED IRM(s)/SUBSECTION(s): 25.23.12

CHANGE(s):

IRM 25.23.12.2(5) Updated Chart to include new digital Form 14039 available on irs.gov. (6) Added U.S. Department of Justice (DOJ) investigation and prosecution information when taxpayer asks for information about finding and prosecuting identity thieves. (7) Added a row when callers inquire about transcripts and identity theft to refer to IRM 21.2.3.5.8, Transcripts and Identity Theft.

(5) Once you have determined the issue and performed the necessary authentication, ask if the taxpayer would prefer to receive identity theft information via the internet or over the phone.

If	Then
Taxpayer prefers to access via the internet	1. Provide the IRS website, irs.gov, 2. Advise the taxpayer to search using key words, "identity theft central". If there are no further issues or questions, go to (6).
Taxpayer states internet access is not an option, or they prefer to receive the resource information over the phone	Provide the following recommendations as applicable: 1. Advise the taxpayer they must continue to file their tax returns and pay the taxes as appropriate while their identity theft claim is under review. 2. Advise the taxpayer they should contact their financial institution to report the allegation of identity theft. 3. Advise the taxpayer to check their local state agencies to determine if additional steps are required at the state level. 4. Advise the taxpayer there may be a few situations where they would also file a report with their local or state police. (i.e., If they know the identity thief or have other information that could help a police investigation, Or if the identity thief used their name during a traffic stop, any encounter with the police, or, if a creditor, debt collector,

	or someone else affected by the identity theft insists the victim provide a police report. 5. Advise the taxpayer to contact one of the three major credit bureaus listed below and provide the web address and contact phone number. They will assist them in identifying what specific information is needed to pursue an allegation of identity theft. o Equifax www.equifax.com 800-525-6285 o Experian www.experian.com 888-397-3742 o TransUnion www.transunion.com 800-680-7289 6. Advise the taxpayer they may contact the two agencies listed below if they are concerned about protecting their identity (including their SSN) to prevent misuse. Provide the web address and contact phone number. The agencies will assist them in identifying what specific information is needed to pursue an allegation of identity theft. o Federal Trade Commission (FTC) www.identitytheft.gov 877-438-4338 **Note:** For victims needing to complete Form 14039, the IRS is currently providing an on-line Form 14039 at https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/ on IRS.gov. This is in addition to the fillable FTC Form 14039 available at identitytheft.gov. This is authorized by the IRS and its present placement on the FTC site is intended as providing an additional resource for identity theft victims who are self-reporting to the FTC. The victim should only file one Form 14039, either directly with the IRS or through the FTC. CSR's should not attempt to provide assistance with the functionality of the FTC website. See IRM 25.23.2.2.1, Taxpayer Interaction. o Social Security Administration (SSA) www.ssa.gov (type in **identity theft** in the search box) 800-772-1213 7. Advise the taxpayer Publication 5027, Identity Theft Information for Taxpayers provides the above resource

	information in English, Spanish, and Braille. This publication and other publications can be obtained electronically on the IRS website, www.irs.gov. **Note:** There are numerous websites and publications available to the public to assist with the prevention of becoming a victim of identity theft and with steps on how to protect personal identifying information (PII) etc. The recommendations above are not all inclusive. If the caller mentions or questions other websites or publications, simply provide a word of caution to ensure the website they are referencing is legitimate. 8. Provide the caller with the identity theft toll-free number including the hours of operation located in paragraph (1) above when appropriate.

(6) If the taxpayer asks for information about the investigation or prosecution of an identity thief, tell them the U.S. Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation (FBI), the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases. Schemes to commit identity theft or fraud may involve violations such as identification fraud, credit card fraud, computer fraud, mail fraud, wire fraud, or financial institution fraud. Each of these federal offenses are felonies that carry substantial penalties and, in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture. If the taxpayer would like additional information, refer them to www.justice.gov. Advise the taxpayer to search using the key words “identity theft”.

(7) Each situation needs to be researched to determine if there is an impact to the taxpayer's account. Refer to If/And/Then chart below:

Note: See Exhibit 25.23.1-1, Glossary of Identity Protection Terms and Definitions, and IRM 25.23.2.4.1, Tracking and Reporting Identity Theft Cases - Identity Theft Indicators, to assist with your determination.

If the Caller’s inquiry is about	**And**	**Then**
Non-Tax-Related	Self-identified identity theft issues	Refer to IRM 25.23.12.3, Non-Tax Related Identity Theft - Self Identified
Tax-related	Identity Theft	Refer to IRM 25.23.12.4, Tax Related Identity Theft
Dependent	Identity Theft	Refer to IRM 25.23.2.3.1, Dependent Identity Theft

		Note: If during a call your research determines their is an open identity theft case, refer to IRM 25.23.4.8.3, Dependent Related Identity Theft (IDT) - General.
IP PIN Program	• Ways to Enroll • Status of application (Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN)) • Non-Receipt, lost, or misplaced	Refer to IRM 25.23.12.6, IP PIN Program Telephone Inquiries
Transcripts	Identity Theft	Refer to IRM 21.2.3.5.8, Transcripts and Identity Theft.

IRM 25.23.12.3(1) Added guidance when accessing a taxpayer's account is not necessary when responding to a non-tax related question only.

(1) Individuals experiencing non-tax-related identity theft may call the IRS for guidance (lost or stolen wallet, fraudulent unemployment claims, etc). Review and research of the taxpayer's account is **not** necessary if non-tax related identity theft guidance is the **only** issue the taxpayer is experiencing. It is important to identify the issue and/or the reason the taxpayer is calling (IP PIN issue, balance due notice, refund offset, rejected e-file, other open issues, etc.) and follow those IRM guidelines.

Note: If the taxpayer is inquiring about phishing and other scams, refer to IRM 21.1.3.23, Scams (Phishing) and Fraudulent Schemes.

IRM 25.23.12.4(1) Added IDT7 to list of open identity theft controls in 2nd Note. (5) Added a new paragraph when taxpayers are calling for the status of their Form 4506-F request and there is an open IDT7 to refer to IRM 25.23.12.5. (7) If and Then chart updated to include new digital Form 14039 available on irs.gov. (10) Updated timeframe from 430 days to 480 days. (11) Updated bullet 1 to include new digital Form 14039 available on irs.gov.

(1) When taxpayers call to report tax-related identity theft, probe the taxpayer to determine if they received a notice or a bill related to unknown income, or received notification of an audit. Review and research the taxpayer's account to determine if additional information is needed. Refer to IRM 25.23.2.3, Identity Protection and Victim Assistance - General Guidelines, and IRM 25.23.2.3.6, When to Request Additional Information to Support an Allegation of Identity Theft, for guidance on when a taxpayer should submit a claim and when additional information is needed. See Exhibit 25.23.1-1, Glossary of Identity Protection Terms and Definitions, for the definition of an "Identity Theft Claim".

Note: If compliance is involved with the case, Form 14039 must be submitted with the taxpayers' response.

Exception: For taxpayer inquiries received on the toll-free lines (examples: App 20/21 or 161/162) that meet Taxpayer Protection Program (TPP) criteria (i.e., taxpayer states they received one of the following letters addressed to them, Letter 4883C, Letter 5071C, Letter 5447C or Letter 5747C; or there is an Unpostable 126 RC 0), see IRM 25.25.6.6, Non Taxpayer Protection Program (TPP) Telephone Assistors Response to Taxpayers.

Note: If during your research you find an open identity theft case control such as an IDT(x), IDS(x), (the "x" represents an IDT/S 1, 3, 6, 7, 8, or 9) **or** IDI(x) (the "x" represents an IDI 1, 2, 3, 4, 5, 6, or 9), see IRM 25.23.12.4.1, Telephone Inquiries Regarding Tax-Related Identity Theft Victim Assistance (IDTVA) Cases, for additional information and guidance.

Caution: Do not advise the caller to complete a Form 3949-A, Information Referral, if the caller has identity theft involving misuse of their own TIN (SSN/ITIN), they have a problem related to their own tax return and tax return preparer, or they received a Duplicate TIN soft notice and want to provide information on the other taxpayer claiming the exemption or Earned Income Tax Credit. See IRM 21.1.3.19, Informant Contacts.

Note: If a taxpayer is calling to report the theft of their refund (ex: stolen from their mailbox, mailed to an incorrect address, stolen from their wallet) or, if their refund was deposited to an incorrect account or closed account, refer to IRM 21.4.2, Refund Trace and Limited Payability.

(2) Be empathetic to the taxpayer's issue. Assure the taxpayer that the IRS is committed to working with them to resolve their identity theft issues. Cases such as theirs require complete and thorough research to provide them with a status update and to make a correct determination for case resolution.

(3) If the taxpayer's call is regarding their Economic Impact Payment (EIP) and they are claiming to be a victim of identity theft, see IRM 25.23.12.4.10, Identity Theft - Economic Impact Payments.

(4) If the taxpayer calls regarding an Identity Protection Personal Identification Number (IP PIN) issue such as lost, misplaced, non-receipt, or electronic filing rejection even though they used their IP PIN, refer to IRM 25.23.12.6, IP PIN Program Telephone Inquiries, for guidance on assisting the taxpayer.

(5) If the taxpayer is calling for the status of their Form 4506-F, Request for Copy of Fraudulent Tax Return and there is an open IDT7 on the account, refer to IRM 25.23.12.5, Responses to Requests for copies of Fraudulent Return(s) for Identity Theft Victims.

(6) If the taxpayer received a reject message after attempting to e-file due to the primary and/or secondary TIN(s) having already been used to e-file a return, then advise the taxpayer to file a paper return with a Form 14039, Identity Theft Affidavit, attached. Advise the taxpayer a fillable Form 14039 is available on IRS.gov. Enter AMS narrative by selecting **Identity Theft**; **"TP will file paper return with IDT claim"**.

Note: See IRM 25.23.2.4.4, Initial Allegations or Suspicion of Tax-Related Identity Theft - IMF Identity theft Indicators, when a taxpayer inquiries or suspects Identity Theft (IDT), for additional guidance.

(7) If the taxpayer is contacting IRS about receiving a rejection message after attempting to e-file for a dependent's TIN, follow procedures in IRM 25.23.12.2 (2) If and Then Chart to authenticate the taxpayer and minor dependent. Ask the taxpayer to confirm the TIN submitted electronically for the dependent matches the information on their social security card or ITIN assignment letter.

If research confirms	Then
1. TIN matches and the dependent's TIN is being used as a primary or secondary TIN on another tax return **Reminder:** Do not disclose information on the return filed under the dependent's TIN.	1. Advise the taxpayer they would need to file a paper return. 2. Advise a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. For victims needing to complete Form 14039, the IRS is currently providing an on-line Form 14039 at https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/ on IRS.gov. 3. Enter AMS and select **Identity Theft**, then enter narrative "**TP will file paper return and advised the dependent should file Form 14039 IDT claim.**" 4. If a dependent's TIN is being used on another return fraudulently and taxpayer will file Form 14039, follow the procedures in IRM 25.23.2.4.4, Initial Allegation or Suspicion of Tax-Related Identity Theft - IMF Identity Theft Indicators, for the input of TC 971 AC 522. 5. Continue with the call following procedures below.
2. The dependent's TIN is being used as a dependent on another tax return and they received a reject message after attempting to e-file. **Reminder:** Do not disclose information on the return the	1. Advise the taxpayer they would need to file a paper return. 2. Inquire if there is another Individual beside the parent/legal guardian who may be claiming this dependent. o If the answer is no, advise the taxpayer a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. For victims needing to complete Form 14039, the IRS is currently providing an on-line Form 14039 at https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/ on IRS.gov. Enter AMS

dependent was claimed on.	and select **Identity Theft**, then enter narrative "**TP will file paper return and advised the dependent should file Form 14039 IDT claim.**" ○ If the answer is yes, provide the caller with options available for the dependent to protect their TIN by filing Form 14039, the IRS is currently providing an on-line Form 14039 at https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/ on IRS.gov or Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN). Enter AMS and select **Identity Theft**, then enter narrative **"TP will file paper return and advised of options available to protect dependent's TIN."** **Reminder:** IDTVA employees are not making a determination regarding which parent/legal guardian is entitled to claim and/or represent the dependent. 3. Advise a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. 4. Follow procedures in IRM 25.23.2.4.4, Initial Allegation or Suspicion of Tax-Related Identity Theft - IMF Identity Theft Indicators, for inputting a TC 971 AC 522 if the taxpayer states they will be filing a Form 14039. If there is no established entity and you receive a response of "No Account on TIF" then enter these additional case notes on AMS when selecting **Identity Theft** in (2) above: **"No established account on TIF - TP PNDCLM DEP IDT"**. 5. Continue with the call following procedures below.

For general information on Dependent Related Identity Theft (IDT), refer to IRM 25.23.4.8.3 and IRM 25.23.2.3.1, Dependent Identity Theft.

(8) If the taxpayer is responding to an IRS letter or notice (with the exception of the TPP letters referenced above), advise the taxpayer to submit an identity theft claim, when appropriate, with a copy of the IRS letter or notice. Send the information to the address indicated on the letter or notice. Enter AMS narrative by selecting **Identity Theft**, "**TP will respond to letter/notice with IDT claim.**"

Reminder: Advise the taxpayer to include any additional information such as written statements, supporting evidence, credit bureau letters etc. the notice/letter is requesting (example: an AUR notice may include a request that all income issues be addressed and whether they are part of the identity theft impact).

Reminder: If the taxpayers call about an IRS balance due issue on a new identity theft claim refer to IRM 25.23.12.4.7, Identity Theft – Balance Due Issues and IRM 5.19.21.2.1, Identity Theft Claim.

(9) Advise the taxpayer there will be processing delays while the situation is resolved and they may receive correspondence requesting additional information.

(10) Provide taxpayers with a realistic expectation of the time frame for resolution of their cases. Explain that identity theft is complex in nature and constantly changing. Apologize to the taxpayer for the length of time required to resolve their issue. Suggested language is:
I apologize for the length of time it is taking to resolve your case. Identity theft is a challenging and ever-changing issue and we are working with victims like you to resolve tax-related identity theft cases. Most cases are resolved in 120 days or less but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically. On average it is taking us 480 days to resolve identity theft cases. We take identity theft seriously and are committed to resolving identity theft cases as quickly as possible and are taking steps to reduce this timeframe. You will receive notification once your case has been resolved.

(11) Individuals not required to file a return may also be negatively impacted by tax-related identity theft. For example, a taxpayer may state the Social Security Administration (SSA) has reduced or stopped their Social Security benefits based on a tax return filed with the IRS. The taxpayer indicates that they have not filed a return. When this type of call is received, follow the instructions below:

- Advise the taxpayers to submit a claim using the on-line Form 14039, currently available on IRS.gov at https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/ on IRS.gov. Include an explanation of their situation. If the taxpayer has any additional information they may think would be appropriate to substantiate their situation, provide the taxpayer with the alternative option of either mailing or faxing their claim. If mailing claim, provide the IRS address associated with the taxpayer's state. Refer to the Campus Mailing Address under the Who/Where tab on Servicewide Electronic Research Program (SERP) for Campus mailing address. If taxpayer chooses to fax their claim, advise them to follow the faxing instructions provided on the second page of Form 14039. Enter AMS narrative and select Identity Theft; **"NFR - TP will respond to letter/notice with IDT claim."**
- Advise the taxpayer they may receive correspondence requesting additional information.

Note: If the taxpayer states they are experiencing an economic hardship because of this event, refer to IRM 21.1.3.18, Taxpayer Advocate Service (TAS) Guidelines.

IRM 25.23.12.4.1(1) Added IDT7 to list of tax-related identity theft controls. (3) Edited guidance to see IRM 21.2.3.5.8, Transcripts and Identity Theft when taxpayers ask about their own transcript information. (7) Updated Note changing "last year" to "last couple years" to account for time lapse and updated timeframe from 430 days to 480 days.

(1) A tax-related identity theft case controlled on IDRS can be identified by control categories, IDT(x), IDS(x) (the "x" represents an IDT/S 1, 3, 6, 8, or 9), **or** IDI(x) (the “x” represents an IDI 1,3, 4, 5, 6, 7, 8 or 9). A telephone CSR **must not** adjust or take any account actions on these **open** identity theft accounts except when the account meets Taxpayer Protection Program (TPP) criteria. Refer to IRM 25.25.6.6, Non Taxpayer Protection Program (TPP) Telephone Assistors Response to Taxpayers.

(2) Basic and high-risk authentication must be completed using the IAT Disclosure tool for all telephone calls when the tool alerts the CSR of an IDT indicator on the account involving open, unresolved, closed, or resolved IDTVA tax related identity theft cases. See IRM 21.1.3.2.3, Required Taxpayer Authentication. If IAT Disclosure tool is not available or an employee has a problem with the IAT Tool Manager, the case should be processed through IDRS following established procedures. See IRM 21.2.2.4.4.14 (2), Integrated Automation Technologies, for additional information.

(3) If the identity theft case is **closed or resolved**, you may provide account information to the TIN owner after authenticating them. You may provide the TIN owner with the information from their account only. Fraudulent information may be combined with the TIN owner's information, such as IRP data, account transcripts, etc. Do not provide information from the fraudulent return. If the taxpayer is asking for their own transcript information see IRM 21.2.3.5.8, Transcripts and Identity Theft. Also refer to IRM 21.2.3.5.8.4.3, Wage and Income Transcript Identity Theft and IRM 25.23.2.10, Get Transcript Breach. You can usually identify the following transaction(s) on Integrated Data Retrieval System (IDRS) via cc ENMOD and/or cc IMFOLE, if the case is resolved.

- A posted TC 971 AC 501 or
- A posted TC 971 AC 506

See IRM 25.23.2.4.1, Tracking and Reporting Identity Theft Cases - Identity Theft Indicators, for additional information related to IDT indicators.

Note: Accounts or cross-reference accounts with TC 971 AC 501, 506, 522, 524 or 525 will not be able to receive transcripts via online, mail order or phone services. Taxpayers are instructed to contact the IDT toll free number for the transcript. Do not refer the taxpayer to self-serve options. See IRM 21.2.3.5.8, Transcripts and Identity

Theft, for additional guidance. For guidelines on issuing a specific type of transcript see IRM 21.2.3.5.8.4, Type of Transcript Requested for Identity Theft Accounts.

Note: # [redacted] **#**

Note: Because there may be instances where an AC 501 or AC 506 is prematurely placed on an account, careful and complete research must be conducted to ensure all actions to resolve the identity theft issue are taken. (EX: CP 01, Letter 4674C, or Letter 239C has been issued to the taxpayer.)

(4) For a closed identity theft case, if the **SSN owner** did not receive their refund, received an incorrect refund amount, or received an incorrect balance due notice because the case is worked incorrectly, (for example, an employee failed to input the TC 971 AC 850 causing a direct deposit into the bad taxpayer's account), treat the case as priority work and take the following actions:

If the case	Then
1. Can be resolved over the telephone, see IRM 21.1.3.20, Oral Statement Authority, and IRM 21.5.2.4.2, Adjustments with Oral Statement	Input the adjustment.
2. Cannot be resolved over the phone and the case meets: • TAS criteria, see IRM 13.1.7.3.1, TAS Case Criteria 1-4, Economic Burden	Complete the correct referral to TAS following guidance in IRM 21.1.3.18, Taxpayer Advocate Service (TAS) Guidelines.
3. Cannot be resolved over the telephone and case does not meet TAS Criteria 1 - 4, Economic Burden criteria	Use IRM referral criteria located in IRM 21.3.5-1, Referral IRM Research List, to refer the taxpayer's issue to the specific employee who previously closed the case. Prepare a Form 4442 following procedures in IRM 21.3.5.4.1, When to Prepare a Referral. Transmit or fax Form 4442 to the specific area based on the AM Case Referral/Reassignment Listing located on SERP.

Reminder: If there is an issue with when to update a taxpayer's address and what can be updated, refer to IRM 25.23.2.3.7, When to Update the Victim's Address.

(5) On **open identity theft cases**, do not give out specific account information on the common TIN (when staffing the toll-free lines) unless the caller passes

additional/high-risk authentication. For additional information, see IRM 21.1.3.2.4, Additional Taxpayer Authentication. If the caller passes the additional taxpayer authentication, you can provide general information on status updates and information from CII case notes entered on "AMS". Provide a reasonable time frame necessary to complete the processing of the case, general information from the case may be necessary. Fraudulent information may be combined with the TIN owner's information, such as IRP data, account transcripts, etc. Do not provide information during the call from the fraudulent return when there is an open identity theft case. You must document AMS with any information provided to the taxpayer during the call.

Caution: Do not assume that the caller is the true owner of the TIN. If, while completing authentication and/or additional authentication, you are unable to determine that you are speaking with the true owner of the TIN, advise the caller to check their records, terminate the call and use AMS issue/narrative to leave a brief note recording the failed disclosure.

(6) If the taxpayer is calling for the status of their transcript request, Form 4506, Request for Copy of Tax Return, or Form 4506-F, Identity Theft Request for Copy of Fraudulent Tax Return, **and** received the **Form 14611**, RAIVS/IVES IPSU, from the RAVIS unit, refer to IRM 25.23.12.4.5, Identity Theft - Transcript Request.

(7) If the taxpayer is calling only to check on the status of their refund and no additional information is provided, then provide an update on the status of the case including a reminder of the identity theft time frames. In an attempt to minimize frustration a statement like this one could be provided:
"*Identity theft is a challenging and ever-changing issue and the IRS is committed to working with victims like you to resolve tax-related identity theft cases. Most cases are resolved in 120 days or less, but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically and on average it is taking us 480 days to resolve identity theft cases. The IRS takes identity theft seriously and is committed to resolving identity theft cases as quickly as possible and are taking steps to reduce this timeframe. You will receive notification once your case has been resolved.*"

Note: If the time frame above has elapsed, apologize to the taxpayer and explain the processing delays due to challenges faced over the last couple years. See IRM 25.23.2.2.3, IDT Case Processing Time Frames.

Reminder: If the taxpayer has not yet filed a return and tax-related identity theft is indicated, see IRM 25.23.12.4, Tax-Related Identity Theft.

IRM 25.23.12.4.5(1) Edited to include guidance specific to the taxpayer's own filed return transcripts. Added If/And/Then chart for the status of transcript requests with and without the receipt of a Form 14611 from RAIVS/IVES.

(1) Refer to IRM 21.2.3.5.8, Transcripts and Identity Theft, for guidance specific to requests involving the taxpayer’s file return(s) and accounts with identity theft. Refer

to IRM 25.23.12.5 when the taxpayer requests a copy of the fraudulent tax return. Refer to the table below when the taxpayer is calling for the status of their request for a copy of a tax return.

If	And	Then
Taxpayer is calling for the status of their request for a copy of a tax return filed on • Form 4506, Request for Copy of Tax Return or • Form 4506-F, Identity Theft Victims Request for Copy of Fraudulent Tax Return	They **did** receive the Form 14611, RAIVS/IVES Additional Actions Needed.	Refer to IRM 21.3.6.4.3.2, Return Copy Procedures and Identity Theft for additional guidance.
Taxpayer is calling for the status of their request for a copy of the fraudulent return filed on Form 4506-F,	They **did not** receive the Form 14611 from RAIVS/IVES.	Refer to IRM 25.23.12.5, Responses to Requests for copies of Fraudulent Return(s) for Identity Theft Victims.

IRM 25.23.12.5(2) Updated timeframe from 430 days to 480 days. (3) Added paragraph with an If/And/Then chart when the taxpayer requests the status of their Form 4506-F fraudulent return request, they did not receive a Form 14611 and there is an open IDT7 on the taxpayer's account.

(2) When an identity theft victim requests a copy of a fraudulent return filed under their SSN via toll-free call, employees will:

- Advise the requestor a Form 4506-F, Identity Theft Victims Request for Copy of Fraudulent Tax Return, is required. Ask if the requestor would prefer to receive the information via the internet or over the phone.
- If the requestor prefers to access the information via internet, then advise that Form 4506-F (with instructions on the back) is available on the IRS website, www.irs.gov, by searching using the form number. Advise the requestor of the FAQs available on www.irs.gov using key words, “identity theft” to search for answers to Frequently Asked Questions regarding identity theft.
- Provide verbally to the requestor who prefers to obtain the information over the phone the information from the IRS website: Instructions for Requesting Copy of Fraudulent Returns.
- Answer any Non-Tax Law question the caller may have about the form and/or instructions.
- Explain the form can be mailed or faxed (not both) and then provide the centralized address and fax number:
  Internal Revenue Service
  Fresno, CA 93888-0025

or
Include a fax cover sheet marked "Confidential"
Fax this form toll-free to 855-807-5720

Note: If the taxpayer is using a private delivery service (examples: FedEx or UPS etc.) a street address must be provided;
3211 S Northpointe Dr.
Fresno, CA 93725
"Identity Theft - Request for Fraudulent Return"

- Inform the requestor some information on the fraudulent return is redacted or blacked out, but there is enough information to determine how the taxpayer's personal information is used.
- Explain the IRS cannot provide a copy of the fraudulent return to any person only listed as a dependent, nor can it be provided to that person's/dependent's parent, legal guardian, or authorized representative.
- Advise the taxpayer most cases are resolved in 120 days or less, but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically and on average it is taking us 480 days to process these requests. The IRS takes identity theft seriously and is committed to resolving their request as quickly as possible and are taking steps to reduce this timeframe.
- Answer any additional questions raised by the requestor; do not refer the taxpayer to another phone number.

(3) When the taxpayer is calling for the status of their Form 4506-F, Request for Copy of Fraudulent Tax Return, and they **did not** receive a Form 14611, RAIVS/IVES IPSU, follow the guidance in the chart below.

If	And	Then
There is an open IDT7 on the taxpayer's account.	There is an open tax-related identity theft as indicated by • open IDT(x), IDS(x) (the "x" represents an IDT/S 1, 3, 6, or 8) Or • open IDI(x) (the "x" represents an IDI 1, 3, 4, 5, 6, 8 or 9). Or • an unreversed TC 971 AC 522 with the MISC field	Refer to IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA)Tax-Related Cases.

	code containing UNWORK	
There is an open IDT7 on the taxpayer's account	There is no open tax-related identity theft case and there is resolved IDT as indicated by • A posted TC 971 AC 501 or • A posted TC 971 AC 506 or There is no indications of tax-related IDT on the account	Advise the taxpayer most cases are resolved in 120 days or less, but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically and on average it is taking us 480 days to process these requests. **Note:** If the time frame above has elapsed and a 5835C Letter has not been sent, apologize to the taxpayer and explain the processing delays due to challenges faced over the last couple years. See IRM 25.23.2.2.3, IDT Case Processing Time Frames. **Note:** If a 5835C Letter has been sent, regardless of timeframe, see paragraph 8 of IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA)Tax-Related Cases, to provide IDTVA employee contact information.

IRM 25.23.12.6.1(2) Updated timeframe from 430 days to 480 days.

(2) When a taxpayer calls to inquire about the IP PIN paper application process, employees will:

- Advise the taxpayer a Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN), is required. Form 15227 is available online for taxpayers or they may call to request a copy at 800-829-3676. Information is also available on line: IRS Forms.
- If the taxpayer prefers to view the information online for how the IP PIN paper process works, advise the taxpayer the information can be found on the IRS website at www.irs.gov. Advise the taxpayer to search using key words "IP PIN" or "Form 15227" for a list of options available to apply for an IP PIN including the Form 15227 IP PIN paper process instructions.
- If the taxpayer does not have access to the internet or prefers to obtain the information over the phone, verbally provide the taxpayer with the filing requirements for submitting Form 15227 provide the toll-free number they can call and order the form; 800-829-3676.

Reminder: # [redacted]

[redacted] #

- Explain the form can be mailed or faxed (not both) and then provide the centralized address or fax number listed under the Instruction section of Form 15227.

  Note:

Where to mail Form 15227	**Where to fax Form 15227**
If submitting Form 15227 by mail: Department of the Treasury, IRS Fresno, CA 93888-0025 If using a private delivery service (FedEx or UPS), provide the following street address: Department of the Treasury, IRS 3211 S Northpointe Dr. Fresno, CA 93725	If submitting Form 15227 by fax: Include a cover sheet marked 'Confidential' Fax to the toll-free number 855-807-5720

- Advise the taxpayer our online services Do Not provide information on the status of their Form 15227 application. Provide taxpayers with a realistic expectation of the time frame for resolution of their application. Apologize to the taxpayer for the length of time required to process their request. Suggested language is: Most cases are resolved in 120 days or less but due to extenuating circumstances caused by the pandemic our inventories have increased dramatically. On average it is taking us 480 days to process some applications. We are committed to processing your application as quickly as possible and are taking steps to reduce this timeframe.
- Explain to the taxpayer once they have been approved to receive an IP PIN using the Form 15227 process they will receive two notices, a 4403C Letter confirming approval of their application and a Notice CP01A containing their IP PIN, in the next 4 to 6 weeks.
- Answer any additional questions raised by the taxpayer; do not refer the taxpayer to a different toll-free number.

IRM 25.23.12.6.3 Added new subsection to include guidance when taxpayers call with questions about IRS online services and ID.me. Guidance includes where taxpayers can get general information for creating an ID.me account, troubleshooting, and reporting fraudulently created or compromised accounts.

(1) The Internal Revenue Service (IRS) works with ID.me, a credential service provider, to provide authentication and identity verification for taxpayers and tax professionals accessing IRS applications including Online Account, Get Transcript Online, Online Payment Agreement, Tax Pro Account, e-Services, Submit Forms 2848 and 8821 Online, and Get an Identity Protection PIN (IP PIN). Users prove their identity by uploading government documents, taking a video selfie, and filling out personal information. These identity verification services are crucial for the IRS to ensure millions of taxpayers and tax professionals can securely access IRS online services.

Note: If taxpayers have an ID.me account from a state government or federal agency, they can sign in without verifying their identity again.

(2) IRS employees cannot assist taxpayers in creating an ID.me account. Do not refer taxpayers to the Electronic Products & Services Support (EPSS) help desk for assistance with creating an ID.me account.

(3) Taxpayers having trouble accessing or creating an account for an IRS online service can visit How to Register for Certain Online Self-Help Tools or should be directed to the IRS ID.me Help Center website by visiting https://help.id.me and selecting Internal Revenue Service located in the “Explore by partners” help section under the “Government” tab.

Note: Taxpayers verifying through video chat must return to IRS.gov to access the online service upon successfully completing the process.

(4) Follow the chart below when a taxpayer reports an ID.me account was created fraudulently, or their account was compromised.

If	And	Then
Taxpayer is reporting an ID.me account was created fraudulently or their account was compromised	They **did** receive a CP 303 notice from the IRS.	• Advise the taxpayer to immediately call the number provided on their CP 303 notice. • Advise them once their identity has been verified their online account will be disabled.
Taxpayer is reporting an ID.me account was created fraudulently or their account was compromised	They **did not** receive a CP 303 notice from the IRS	Advise the taxpayer to immediately report it to ID.me. Refer them to the Privacy & Fraud section of the ID.me Help Center. Taxpayers can use key words “reporting identity fraud” in the search section for steps to report the suspected fraud.

(5) Information for ID.me can be found in IRM 21.2.1.58.2, Secure Access Digital Identity (SADI). Also, refer to IMF eAuthentication Job Aid available in the Job Aids

section of the Servicewide Electronic Research Program (SERP). This job aid provides a visual tutorial for creating a new ID.me account.